

G202 Industrial Edge Computing Gateway



User Manual

Version: 1.5

© Vantron Technology, Inc. All rights reserved.

Revision History

No.	Software Version	Description	Date
V1.0	V200R003	First release	Jun. 21, 2021
V1.1	V200R003	1. Added description of OpenVPN Server 2. Modified DMP Agent and RC to PLC	Jan. 19, 2022
V1.2	V200R003	Modified 3.5.3 4G/LTE	Apr. 12, 2022
V1.3	V200R003	Updated contact information	Jun. 15, 2022
V1.4	V200R003	Updated serial port description	Oct. 10, 2022
V1.5	V200R003	Updated hardware connection	Nov. 18, 2022

Table of Contents

Foreword	1
CHAPTER 1 INTRODUCTION	5
1.1 Product Overview	6
1.2 Packaging Checklist.....	7
1.3 Specifications.....	8
1.4 Definition of Interfaces.....	9
1.5 Serial Port Introduction	12
CHAPTER 2 GETTING STARTED	13
2.1 Setting up the Gateway	14
2.2 Gateway Login	16
2.3 Connection to Vantron Gateway Management Platform	17
2.4 Network Connectivity.....	17
2.4.1 Ethernet Network Connectivity.....	18
2.4.2 Wi-Fi Connectivity	18
2.4.3 Mobile Network Connectivity	18
2.5 Custom Settings.....	18
CHAPTER 3 GATEWAY CONFIGURATION.....	19
3.1 Introduction to VantronOS	20
3.2 Status.....	21
3.3 Quick Start.....	23
3.3.1 Network Guide	23
3.3.2 WAN Setting – DHCP	23
3.3.3 WAN Setting – Client	24
3.3.4 WAN Setting – 4G/LTE	25
3.3.5 WAN Setting – PPPoE	26
3.3.6 WAN Setting – Static.....	27
3.3.7 Auto Routing	28
3.4 Virtual Tunnel	30
3.4.1 OpenVPN Server.....	30
3.4.2 VPN Client.....	31
3.5 Network.....	32
3.5.1 Interfaces.....	33
LAN	34
4G	37
WAN	37
3.5.2 Wireless (WIFI)	38
Wi-Fi – AP Mode (General settings)	39
Wi-Fi – AP Mode (Advanced setting).....	40

Wi-Fi – Client Mode.....	41
3.5.3 4G/LTE	42
3.5.4 Static Routes.....	45
3.5.5 Firewall	46
3.6 Customization.....	48
3.6.1 Custom Program.....	49
3.6.2 IPK Installer.....	49
3.6.3 Manufacturer Info Customization	50
3.6.4 DMP Agent	51
3.7 Hardware.....	52
3.7.1 Ser2TCP	52
3.8 Services.....	53
3.8.1 Dynamic DNS.....	53
3.8.2 RC to PLC	54
3.9 System	55
3.9.1 System	55
3.9.2 NBM Setting	56
3.9.3 Administration.....	56
SSH Access	57
3.9.4 Terminal.....	58
3.9.5 Mount Points.....	58
3.9.6 Backup/Flash Firmware	58
3.9.7 Reboot	59
3.10 Logout.....	59
CHAPTER 4 INDUSTRIAL PROTOCOL CONFIGURATION	60
4.1 IPK Installation for Industrial Protocols	61
4.2 Protocol Configuration and Application	62
4.2.1 Configuration of Data Acquisition Protocols	62
4.2.2 Device Configuration.....	64
4.2.3 Add Variables to the Device	65
4.2.4 Edge Computing Scripts Setup	67
5.2.5 Data Upload and Encapsulation	69
4.2.6 Alarm.....	72
4.2.7 Logs	73
4.2.8 System Settings	73
5.1 Disposal	75
5.2 Warranty.....	76
Appendix A Regulatory Compliance Statement	77
APPENDIX B Acronyms	78

Foreword

Thank you for purchasing G202 Industrial Gateway (“the Gateway” or “the Product”). This manual intends to provide guidance and assistance necessary on setting up, operating and maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Intended Users

This manual is intended for:

- Network architects/programmers
- Network administrators
- Technical support engineers
- Other users

Copyright

Vantron Technology, Inc. (“Vantron”) reserves all rights of this manual, including the right to change the content, form, product features, and specifications contained herein at any time without prior notice. An up-to-date version of this manual is available at www.vantrontech.com.

The trademarks in this manual, registered or not, are properties of their respective owners. Under no circumstances shall any part of this user manual be copied, reproduced, translated, or sold. This manual is not intended to be altered or used for other purposes unless otherwise permitted in writing by Vantron. Vantron reserves the right of all publicly released copies of this manual.

Disclaimer

While all information contained herein has been carefully checked to assure its accuracy in technical details and typography, Vantron does not assume any responsibility resulting from any error or features of this manual, nor from improper uses of this manual or the software.

It is our practice to change part numbers when published ratings or features are changed, or when significant structure changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please include the following information in your question:

- Product name and PO number;
- Complete description of the problem;
- Error message you received, if any.

US Office: Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information



The Product is designed to comply with:

- Part 15 of the FCC Rules;

Please refer to **Appendix A** for Regulatory Compliance Statement.

Symbology

This manual uses the following signs to prompt users to pay special attention to relevant information.







	Caution for latent damage to system or human injury
	Attention to important information or regulations

General Safety Instructions

The Product is supposed be installed by knowledgeable, skilled persons familiar with local and/or international electrical codes and regulations. For your safety and prevention of damage to the Product and other equipment connected to it, please read and observe carefully the following safety instructions prior to installation and operation. Keep this manual well for future reference.

- Do not disassemble or otherwise modify the Product. Such action may cause heat generation, ignition, electronic shock, or other damages including human injury, and may void your warranty.
- Keep the Product away from heat source, such as heater, heat dissipater, or engine casing.
- Do not insert foreign materials into any opening of the Product as it may cause the Product to malfunction or burn out.
- To ensure proper functioning and prevent overheating of the Product, do not cover or block the ventilation holes of the Product.
- Follow the installation instructions with the installation tools provided or recommended.
- The use or placement of the operation tools shall comply with the code of practice of such tools to avoid short circuit of the Product.
- Cut off the power before inspection of the Product to avoid human injury or product damage.

Precautions for Power Cables and Accessories

-  Use proper power source only. Make sure the supply voltage falls within the specified range. The Product is designed to use 9-36V DC. Always check whether the Product is DC powered before applying power.
-  Place the cables properly at places without extrusion hazards.
-  Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.
-  Cleaning instructions:
 - Power off the Product before cleaning
 - Do not use spray detergent
 - Clean with a damp cloth
 - Do not try to clean exposed electronic components unless with a dust collector
-  Power off and contact Vantron technical support engineer in case of the following faults:
 - The Product is damaged
 - The temperature is excessively high
 - Fault is still not solved after troubleshooting according to this manual
-  Do not use in combustible and explosive environment:
 - Keep away from combustible and explosive environment
 - Keep away from all energized circuits
 - Unauthorized removal of the enclosure from the Product is not allowed
 - Do not change components unless the power cable is unplugged
 - In some cases, the Product may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the Product before replacement of the components.

CHAPTER 1

INTRODUCTION

1.1 Product Overview

Vantron G202 industrial edge computing gateway is an entry-level gateway launched to meet the needs of Industrial IoT applications in various scenarios. It combines dual SIM LTE, Wi-Fi, Ethernet, multiple programming languages, and virtual private network to meet diversified networking requirements. With varying industrial protocols supported, it could interact with PLCs, sensors and other IoT devices on site. G202 applies a communication tactic that uses multiple channels with failover protocol, which together with the high-reliability watchdog maintains a secure and stable network access. As is compact in size, G202 supports panel mount, DIN rail mount, and wall mount to meet the requirements of varying sites. Meanwhile it provides access to Vantron BlueSphere cloud platform for unified management to ease the efforts of users by real-time monitoring and tracking, OTA updates, remote maintenance, task assignment and follow-up.

Featuring high stability and reliability, excellent cost performance, and broad protocol accessibility, G202 industrial edge computing gateway is especially suitable for large-scale data acquisition and cloud platform communication in the following scenarios:

Intelligent manufacturing: injection molding machine, numerical control machine

Intelligent water conservation: water treatment

Intelligent security & intelligent transportation

1.2 Packaging Checklist

The Product has been carefully packed with special attention to quality. However, should you find anything damaged or missing, please contact your sales representative in due time.

Standard accessories:



1 x gateway



1 x power adapter



1 x power cable



2 x Wi-Fi antenna

Optional accessories:




2 x 4G LTE antenna



1 x DIN rail mounting bracket



1 x wall mount bracket

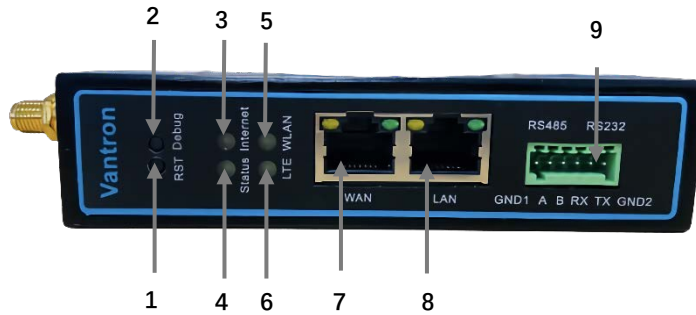
 Actual accessories might vary slightly from the list above as the customer order might differ from the standard configuration options.

1.3 Specifications

G202		
System	Memory	32MB
	Storage	128MB 1 x Micro SD card, up to 64GB
Communication	Ethernet	2 x RJ45, 10/100Mbps
	4G LTE	CAT M/CAT 1/CAT 4
	Wi-Fi	2.4GHz, 802.11 b/g/n, 300Mbps, AP & Client
	Ethernet port protocol	PPP, PPPoE, DHCP, ARP
I/Os	Serial port	1 x RS485 1 x RS485 (default)/RS232, isolated
	SIM slot	2 x Drawer-type SIM slot
	Grounding	Enclosure & PCB
System Control	Button	1 x Reset button 1 x Debug button
	LED	1 x Status
		1 x Internet
		1 x LTE
1 x WLAN		
Mechanical	Dimensions	115.5 x 85.77 x 28.3mm
	Enclosure	Metal
	Installation	DIN rail mount/Wall mount/Panel mount
	IP rating	IP30
	Cooling mode	Fanless
Power	Input	9-36V DC, Over-current protection, Anti-reverse protection
	Terminal	3-pin 3.81mm terminal
Software	OS	VantronOS
	SDK	Available
	Network management	SNMP v1/v2c/v3
	Device management platform	Vantron BlueSphere
	Third-party platform	MQTT
	IPK import	Supported
	Interface language	Chinese and English (Default) Other languages (Optional)
	NTP	Supported
	Log	Supported
	Security	Firewall
Data security		OpenVPN, L2TP, PPTP, IPSec
Link detection		Heartbeat detection, automatic reconnection
Network reliability		Failover, Ethernet Link, Wi-Fi, 4G LTE backup
Multi-level permission		Supported
Application	Configuration mode	Local, remote
	Upgrade	Local, OTA update
	Networking guide	One-key configuration of LTE, Wi-Fi, and Ethernet
	IP application	Ping, Traceroute, Nslookup
	IP Routing	Static routing
	NAT	Supported
Industrial Protocol	Industrial protocol	Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-link, etc.
Edge Computing	Edge computing	Supported by local script
User Programmable	Development language	C/C++/Python
Environment Condition	Temperature	Operating: -20°C ~ +60°C Storage: -40°C~+70°C
	Humidity	RH 5%-95% (Non-condensing)
	Certification	CE, FCC, PTCRB

1.4 Definition of Interfaces

1.4.1 Front view



Button description

No.	Button	Description
1	RST	The gateway will be factory reset with user data and custom configurations erased when this button is pressed for 3-10 seconds. The system will reboot upon reset of the gateway.
2	Debug	Under normal circumstances, the RS485/RS232 multiplexer (labeled as RS232 on the above device) is used for serial communication by default. Long press of the debug button before power application will switch the port to the debug mode. However, when the Gateway is powered off, the port will restore to the communication mode. Refer to 1.5 Serial Port Introduction for details.

LED indicators

1. Internet indicator

No.	Network connectivity of the Gateway	Description
3	Yes	The indicator blinks
	No	The indicator is off

2. Status indicator

No.	System action	Description
4	System bootup	The indicator blinks
	System running properly	The indicator is solid green

3. WLAN (Wi-Fi) indicator

No.	Wi-Fi module status	Description
5	The Wi-Fi module is on	The indicator is solid green
	A client is connected to the Gateway via Wi-Fi	The indicator blinks
	The Wi-Fi module is off	The indicator is off

4. 4G LTE signal strength indicator

No.	4G LTE module status	Description
6	The 4G LTE module is on	The indicator is solid green
	The 4G LTE module is not provided	The indicator is off

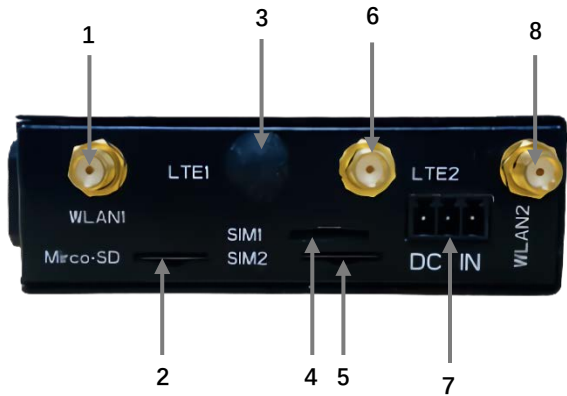
Ethernet ports description:

No.	Port	Description
7	WAN	Set as ETH0.2 in VantronOS and works in WAN area by default
8	LAN	Set as ETH0.1 in VantronOS and works in LAN area by default

Green terminal block:

No.	Port	Description
9	RS485	Used for serial communication
	RS485/RS232	Serial communication by default, serial debugging available

1.4.2 Left side view



Interface	Description
1	WLAN antenna 1
2	Micro SD card slot
3	4G LTE antenna 1
4	Micro SIM card slot 1
5	Micro SIM card slot 2
6	4G LTE antenna 2
7	9-36V DC power terminal
8	WLAN antenna 2

1.4.3 Right side view



Interface	Description
1	Grounding screw

1.5 Serial Port Introduction



There are two serial ports on the terminal block of the Gateway, one is RS485, the other is multiplexed as RS485 or RS232 depending on the requirement of the customer. Users can use the **vtsysinfo** command to figure out which one is currently used.

The multiplexer is used for serial communication by default. To activate the debug mode, users can long press the debug button before power application till output data is displayed on the host PC. When the Gateway is powered off, the port will restore to the communication mode.

However, it is recommended that users do not use the port for serial debugging when the multiplexer is configured to RS485 due to garbled characters in the “copy and paste” process and the need of an RS232 to RS485 adapter.

Pinout description:

No. (Left to right)	Pin	Node name	Port	Type	Definition
1	GND1	/dev/ttyS1	COM1	NC	RS485 isolated grounding
2	A			I/O	RS485-A signal
3	B			I/O	RS485-B signal
4	RX / A	/dev/ttyS0	COM2	I	RS232 RXD signal/ RS485-A signal
5	TX / B			O	RS232 TXD signal/ RS485-B signal
6	GND2			I	Isolated grounding

Input the following command lines in the **Terminal** page of VantronOS or in the host device that can write and read data for serial communication:


1. For RS232/RS485 communication:

```
~# microcom /dev/ttyS0 -s 115200
```

2. For RS485 communication:

```
~# microcom /dev/ttyS1 -s 115200
```

 Please refer to **Appendix B** for the definition of the acronyms mentioned above.

 Please refer to [3.9.4 Terminal](#) for how to open the terminal and input the commands.

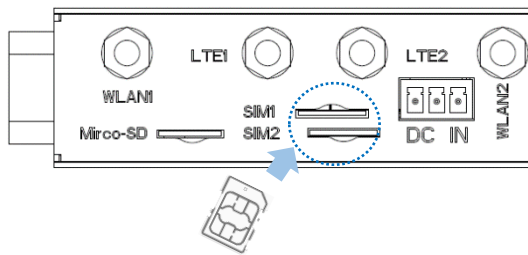
CHAPTER 2

GETTING STARTED

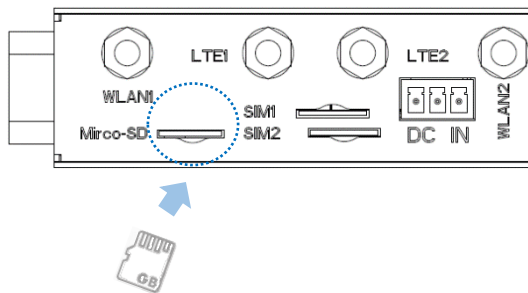
2.1 Setting up the Gateway

Before you proceed with configuration of the Gateway, follow the steps below to finish hardware connection.

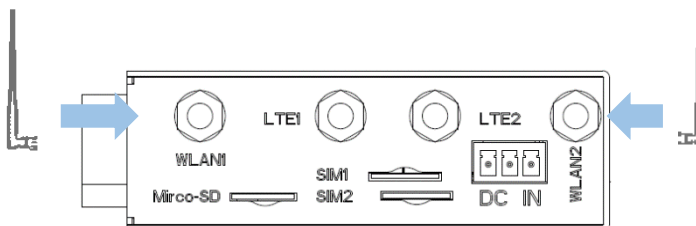
1. Use the mounting bracket and screws provided to install the Gateway to a secure place;
2. Insert an activated SIM card into SIM1 slot with the gold-colored contacts facing down, or, insert into SIM2 slot with the gold-colored contacts facing up;



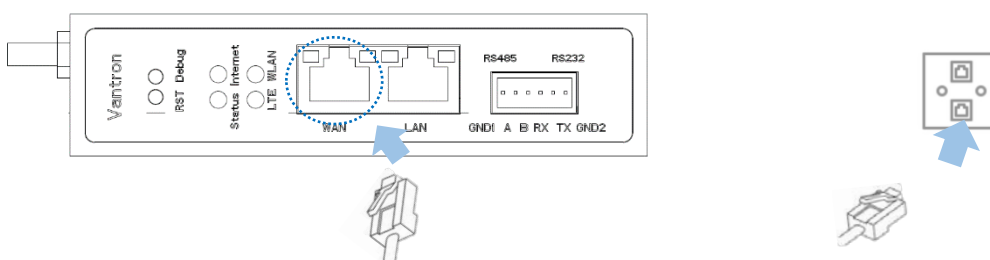
3. Push the SIM card to secure it;
4. Insert a Micro SD card into the Micro SD card slot with the gold-colored pins facing up;



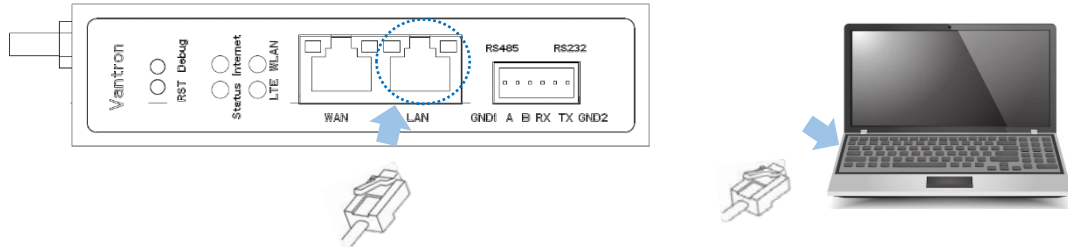
5. Install the round head antennas to the WLAN antenna connectors and the flat head antennas to the LTE antenna connectors;



6. Connect one end of an Ethernet cable to the WAN port of the Gateway and the other to a live Ethernet port;

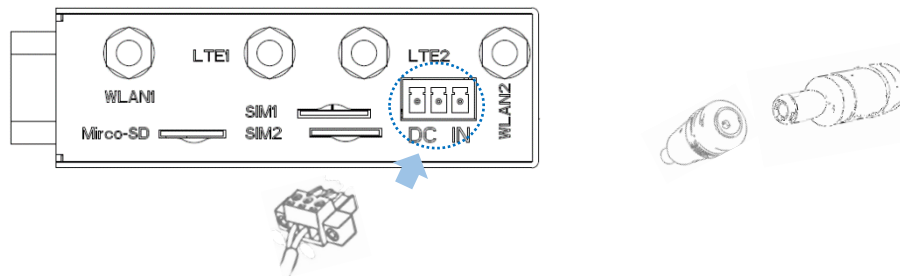


7. Connect one end of an Ethernet cable to the LAN port of the Gateway and the other to your PC;



▶ Skip steps 6 & 7 if you choose wireless network connection.

8. Connect the female connector plug of the power cable to the terminal block of the Gateway and the round end to the adapter;



9. Plug the adapter to a DC power outlet that provides voltage ranging from 9V to 36V to turn on the Gateway;
10. The power indicator will turn solid green upon power application.

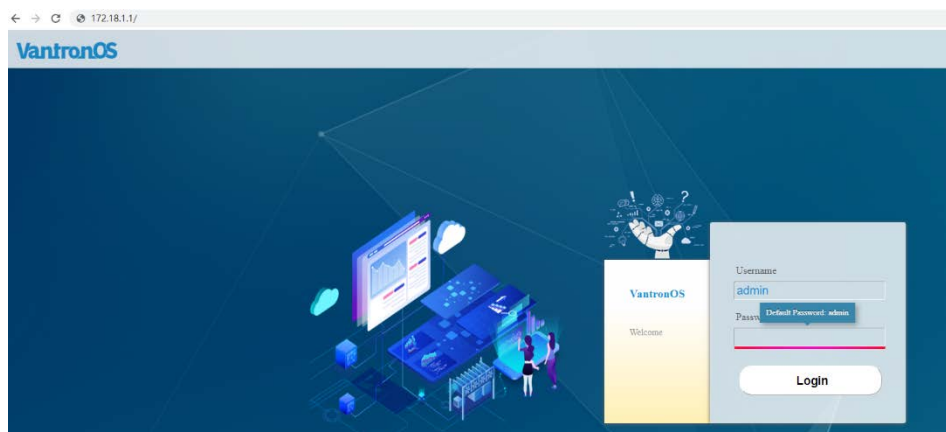
▶ The antenna connectors might vary with the functions. Should you have any trouble installing the antennas, please contact the sales representative for solution.

▶ Customers have the option for 4G LTE module that is AT&T and Verizon pre-certified. Before you use a SIM card to provide wireless network access for the Gateway, make sure the SIM card is activated with data plans (refer to [3.5.3 4G/LTE](#) for the application of the SIM card from the carriers if the module is pre-certified).

2.2 Gateway Login

The Gateway is designed to allow network connectivity with minimal configuration. That said, you can configure the network settings and customize the Gateway from VantronOS interface.

1. Input the default web login address of VantronOS in your browser: <http://172.18.1.1/>.
 - Default user name: **admin**
 - Default password: **admin**



2. You'll be directed to the web interface of VantronOS, and you can make configurations and changes here with VantronOS interface.
3. For SSH login, use the IP address: 172.18.1.1 (default).
 - Port: **22**
 - Account: **root**
 - Password: **rootpassword**

Refer to **SSH Access** included in [3.9.3 Administration](#) for more details.

- ▶ The web login address coincides with the IP address of the Gateway, so you might have to change the login address when you reset the IP address of the Gateway.
- ▶ The latest version of Google Chrome or Firefox is recommended.

2.3 Connection to Vantron Gateway Management Platform

With Vantron gateway management platform, a console where multiple gateways could be managed in groups to provide required information of a target workplace, the Gateway can be monitored and managed remotely.

Refer to [3.6.4 DMP Agent](#) for the configuration. More detailed information is available in the user manual of Vantron gateway management platform.

2.4 Network Connectivity

When the Gateway has both wired and wireless connections, the status page will display like below.



2.4.1 Ethernet Network Connectivity

The default WAN settings allow your gateway to join an Ethernet network without any additional configuration.

The Gateway uses a DHCP protocol to assign IP addresses, subnet masks, default gateway addresses, and Domain Name System (DNS) server addresses by default. If you switch DHCP to static protocol, you'll need to set all the IP addresses manually.

2.4.2 Wi-Fi Connectivity

The Gateway is configurable to both client mode and AP mode.

Refer to [3.5.2 Wireless \(WIFI\)](#) for advanced settings of the wireless network.

2.4.3 Mobile Network Connectivity

For customers using a SIM card for network connectivity of the Gateway, the 4G/LTE function under **Network** tab allows you to make changes to the cellular network settings. Before you configure for 4G/LTE network, be sure to activate and install the SIM card properly.

Refer to [3.5.3 4G/LTE](#) for advanced settings of the mobile network.

2.5 Custom Settings

As Vantron provides an SDK, users can upload their own scripts or programs or IPK packages to the Gateway and set them to run at startup or to support certain protocols.

Refer to [3.6 Customization](#) for advanced settings of customized packages and programs.

CHAPTER 3

GATEWAY CONFIGURATION

3.1 Introduction to VantronOS

Featuring independent development of system and functions, VantronOS is an intelligent operating system that interprets the joint efforts of Vantron team based on Linux system and embedded hardware. It employs modular design and plug-in expansion design ideas, running Linux kernel with firewall to secure Internet connection of devices without being attacked. The UI interface is based on the MVC framework to provide a simple and efficient setting entry. VantronOS also realizes connectivity with cloud management platforms, including self-developed BlueSphere GWM, Azure, Alibaba Cloud, Huawei Cloud, and RootCloud to allow users to monitor, operate and diagnose remote devices without sending technical support engineer to the equipment site, achieving the interconnection and interaction between users and the Industrial Internet of Things.

3.2 Status

This page provides the overall information of the Gateway, including stable operation duration, number of devices connected to the Gateway via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.



Description of the numbered areas

1. Firmware version and auto refresh on/off
2. Stable running time of the Gateway since network connection
3. Current working status of Ethernet ports
4. A collection of network diagnostic tools
5. Instant default exit traffic
6. Model, serial number, and IP address of the gateway in use
7. System log information
8. Kernel log information
9. Number of clients connected to the Gateway via Wi-Fi

Wi-Fi settings will be accessed upon a click of the number.

10. Address information of clients connected to the Gateway

- ▶ ARP scan is disabled by default, and it can be enabled when you click on **arplist** icon and toggle on ARP scan in the pop-up.

ARP Scan: ☐

IPv4-Address	MAC-Address
172.18.1	12:21:d5:11:c5:d0
172.18.1	86:a2:a0:2e:22:43
172.18.1	02:a5:e3:ea:a3:91
172.18.1	f8:c3:9e:97:a4:ff
172.18.1	62:54:8b:61:7f:8a
172.18.1	42:63:de:da:77:85
172.18.1	18:c0:4d:43:ad:8b

11. Details of the access port

- ▶ The image illustration varies when the Gateway has cellular connection.



12. Default route currently used by the Gateway

13. Traffic distribution of clients connected to the Gateway displayed by MAC addresses

- ▶ Clicking on each MAC address in the table at the page bottom will get the detailed traffic information of the clients.

14. Application layer protocols

- ▶ HTTPS, HTTP, and POP3S represent the top 3 protocols for data download and upload.
HTTPS, HTTP and DNS represent the top 3 protocols for device connection.

3.3 Quick Start

3.3.1 Network Guide

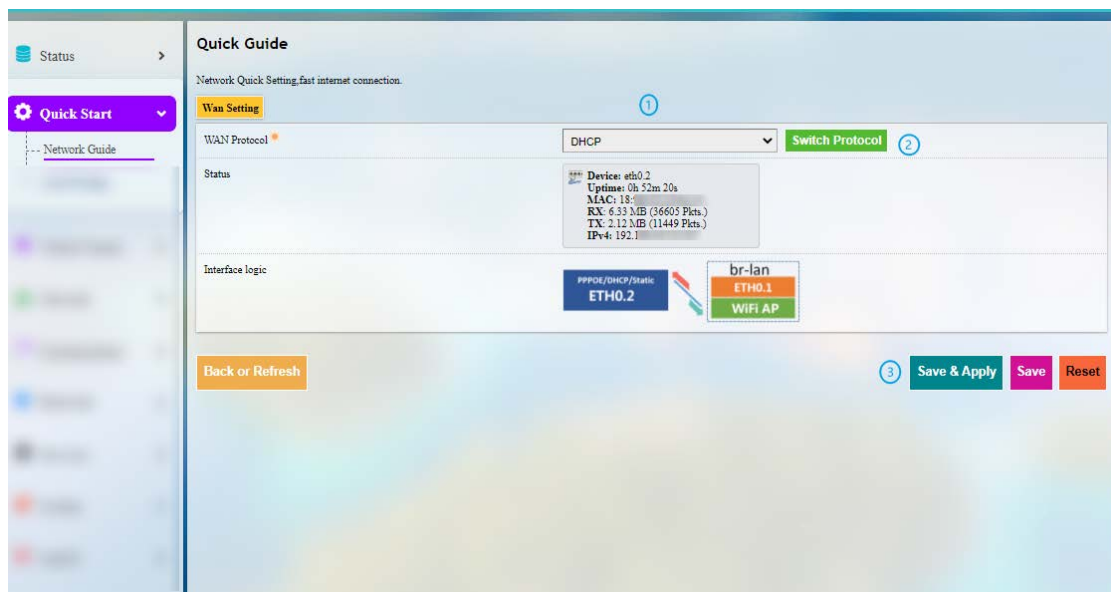
This page provides a quick guide to such functions as rapid networking of the Gateway and a display of the network port status and interface logic diagram. Refer to [3.5.1 Interfaces](#) for advanced settings.

▶ Application of the network setup wizard will clear customer-defined configuration parameters.

▶ Please refer to [1.4 Definition of Interfaces](#) for the definition of the ports.

3.3.2 WAN Setting – DHCP

DHCP: ETH0.1 and **WiFi AP** are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network. The cellular interface does not work under this mode.



DHCP setup procedures:

Step 1: Select **DHCP** for **WAN Protocol**;

Step 2: Click to switch the protocol to **DHCP**;

Step 3: Click **Save & Apply**.

▶ Switch of WAN protocol will reset the network port topology and network parameters to default values.

3.3.3 WAN Setting – Client

Client: ETH0.1 and ETH0.2 are bounded with the network bridge (br-lan). **WiFi Client** is designed as the WAN port to connect the higher-level network.

The screenshot shows the 'WAN Setting' configuration page for a 'Client' protocol. The page includes a 'Quick Guide' section with numbered steps 1 through 9. The form fields are as follows:

- WAN Protocol: Client (Step 1)
- Status: Interface not present or not connected yet (Step 2)
- Interface logic: WiFi Client (Step 3)
- Select SSID: -- Please choose -- (Step 4)
- Scan WIFI: Scan WIFI button (Step 5)
- Mac Bssid: Auto (Step 6)
- Key: (Step 7)
- Internet connection?: Yes (Step 8)
- Protocol: DHCP (Step 9)

At the bottom, there are buttons for 'Back or Refresh', 'Save & Apply', 'Save', and 'Reset'.

Client (Wi-Fi) setup procedures:

- Step 1: Select **Client** for **WAN Protocol**;
- Step 2: Click to switch the protocol to **Client**;
- Step 3: Select the Wi-Fi network that the Gateway is to connect;
- Step 4: Click **Scan WIFI** to refresh the Wi-Fi list if the target Wi-Fi network is not identified;
- Step 5: Select the MAC address of the AP to be connected (leave it to Auto if not certain);
- Step 6: Enter the password of the Wi-Fi network to be connected;
- Step 7: Confirm if the Wi-Fi network is accessible. If not, select **No** as the heartbeat detection method might be different;
- Step 8: Select the protocol for IP addressing (DHCP by default);
- Step 9: Click **Save & Apply**.

3.3.4 WAN Setting – 4G/LTE

Before you configure for 4G/LTE connection, make sure you have inserted the activated SIM card in the slot. Refer to [3.5.3 4G/LTE](#) for advanced settings.

4G/LTE: ETH0.1, ETH0.2 and WiFi AP are bounded with the network bridge (br-lan). Normally, if the Gateway is using a common 4G module, the device port for 4G/LTE communication displayed under the protocol will be “3g-4g” which is the WAN port. When using a carrier pre-certified 4G module provided by Vantron, the device port for 4G/LTE communication displayed under the protocol will be “eth2” which is the WAN port.

The screenshot displays the 'WAN Setting' configuration page. At the top, the 'WAN Protocol' is set to '4G/LTE'. Below this, the 'Interface logic' section shows a diagram where '4G/LTE' is connected to 'br-lan' (ETH0.1/ETH0.2) and 'WiFi AP'. The 'Status' section shows device information: 'Device: 3g-4g', 'RX: 0 B (0 Pkts.)', and 'TX: 0 B (0 Pkts.)'. The 'Dial number' field is set to '*99***1#', 'APN' is '3gnet', 'PAP/CHAP username' is 'your_username', and 'PAP/CHAP password' is masked with asterisks. At the bottom, there are buttons for 'Back or Refresh', 'Save & Apply', 'Save', and 'Reset'. Numbered callouts 1 through 7 highlight key steps in the configuration process.

4G/LTE setup procedures:

Step 1: Select **4G/LTE** for **WAN Protocol**;

Step 2: Click to switch the protocol to **4G/LTE**;

Step 3: Enter the SIM card ICCID provided by the carrier;

Step 4: Enter the APN of the SIM card inserted (provided by the carrier);

Step 5: Enter the username provided by the carrier for PAP/CHAP authentication;

Step 6: Enter the password provided by the carrier for PAP/CHAP authentication;

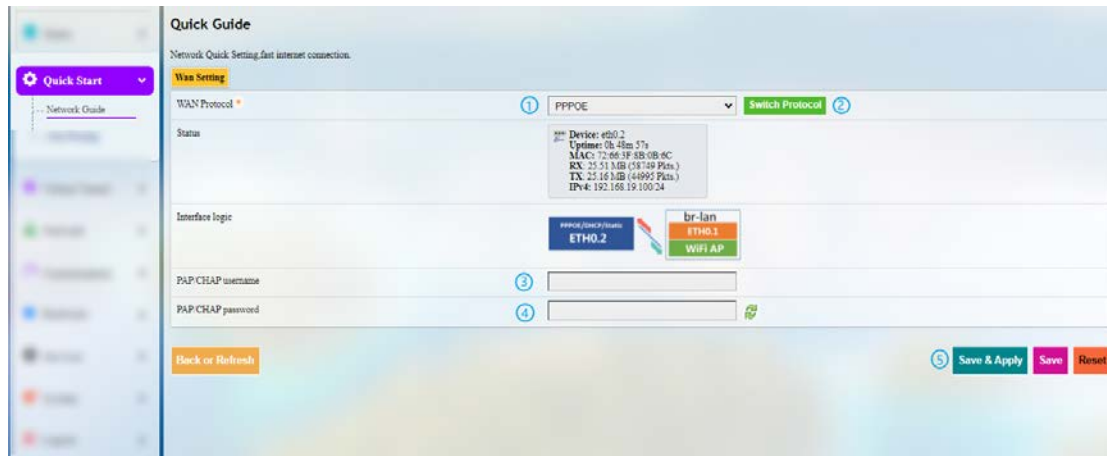
Step 7: Click **Save & Apply**.

Leave the field as is if not available.

PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

3.3.5 WAN Setting – PPPoE

PPPoE: ETH0.1 and WiFi AP are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network.



PPPoE setup procedures:

Step 1: Select **PPPoE** for **WAN Protocol**;

Step 2: Click to switch the protocol to **PPPoE**;

Step 3: Enter the username for PAP/CHAP authentication;

Step 4: Enter the password for PAP/CHAP authentication;

Step 5: Click **Save & Apply**.

3.3.6 WAN Setting – Static

Static: **ETH0.1** and **WiFi AP** are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network.

The screenshot displays the 'WAN Setting' configuration page for a static IP connection. The interface includes a sidebar with 'Quick Start' and 'Network Guide' options. The main content area is titled 'Quick Guide' and 'Network Quick Setting, fast internet connection.' The 'WAN Setting' section shows the 'WAN Protocol' set to 'Static' (Step 1). A 'Switch Protocol' button is available (Step 2). The 'Status' section displays device information for eth0.2: Uptime: 0h 3m 33s, MAC: 18:9B:A5:14:83:13, RX: 788.85 KB (3554 Pkts.), TX: 1.63 MB (2484 Pkts.), and IPv4: 192.168.19.108/24. The 'Interface logic' section shows a diagram with 'PPPoe/DHCP/Static' and 'ETH0.2' connected to a 'br-lan' bridge, which also includes 'ETH0.1' and 'WiFi AP'. The configuration fields are: 'IPv4 address' (Step 3), 'IPv4 netmask' (255.255.255.0, Step 4), 'IPv4 gateway' (Step 5), 'IPv4 broadcast' (Step 6), and 'Use custom DNS servers' (8.8.8.8, 114.114.114.114, Step 7). At the bottom, there are buttons for 'Back or Refresh', 'Save & Apply' (Step 8), 'Save', and 'Reset'.

Static protocol setup procedures:

Step 1: Select **Static** for **WAN Protocol**;

Step 2: Click to switch the protocol to **Static**;

Step 3: Specify the IPv4 address;


Step 4: Specify the subnet mask;

Step 5: Specify the IPv4 gateway;

Step 6: Specify the IPv4 broadcast;

Step 7: Set the DNS server;

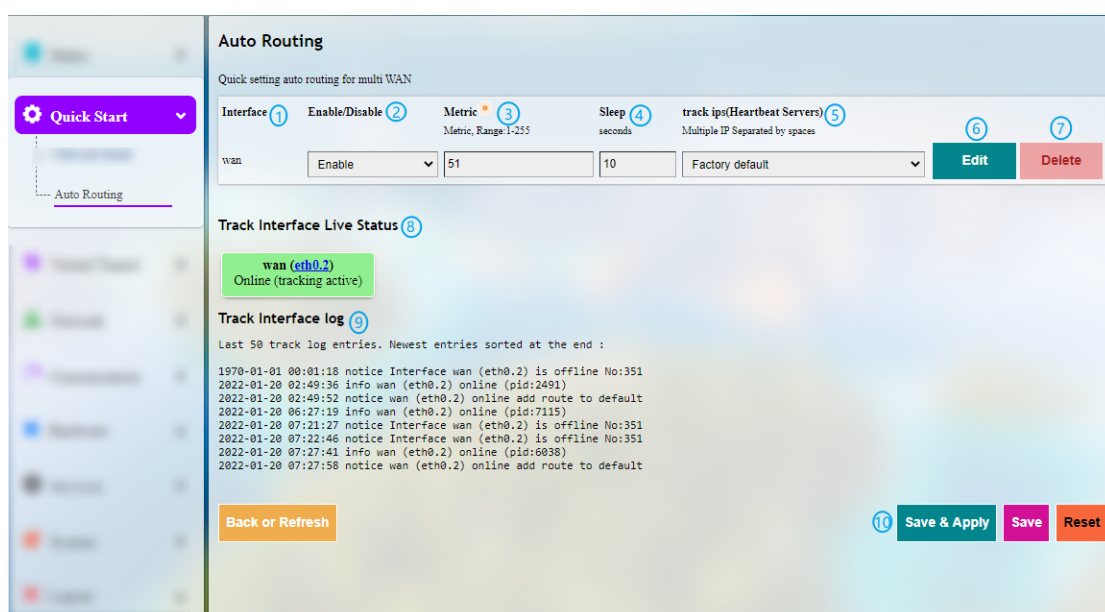
Step 8: Click **Save & Apply**.

 Leave the field as is if not available.

3.3.7 Auto Routing

Automatic routing features functions briefed below:

- Enable heartbeat detection upon connection to a single 4G network interface;
- When there are multiple WAN ports, users can specify the data port according to the metric priority of the Gateway. When one of the ports is offline, auto routing helps automatically switch to other available ports. When the failed port recovers and comes online again, it can automatically re-connect to the network;
- Initiate automatic recognition, add the automatically detected port when a network port plugs in/out.



Description of the numbered areas

1. Interface for route tracking
2. Enable/Disable route tracking
3. Metric settings (The smaller the number, the higher the priority)
4. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking
5. Traceable IP (heartbeat server)
6. Edit rules
7. Delete rules
8. Status overview of interfaces tracked
9. Interface track log with the newest entry at the bottom

10. **Save & Apply** the changes made

Clicking on the **Edit** button will direct you to the rule editing page as follows.

The screenshot shows the 'Advanced Setting' page for route tracking. The settings are as follows:

Setting	Value
Enable/Disable	Enable
Network	wan
Metric	51
Count	2
Timeout	8
Online	2
Offline	4
Sleep	10
track ips(Heartbeat Servers)	Factory default

Buttons at the bottom: Back or Refresh, Save & Apply (circled 10), Save, Reset.

Description of the numbered areas

1. Enable/Disable route tracking
 2. Select the interface for route tracking
 3. Metric settings (The smaller the number, the higher the priority)
 4. The maximum retry number for a single tracking failure
 5. The maximum timeout for a single tracking failure
 6. Number of online interfaces
 7. Number of offline interfaces
 8. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking
 9. Traceable IP (heartbeat server)
 10. **Save & Apply** the settings
- Information:** If a tracking is confirmed successful, the interface will be considered online.
- Information:** If a tracking is confirmed failed and the confirmation number reaches/exceeds the pre-set value, the interface will be considered offline.
- Information:** Use spaces to separate multiple IP addresses. If you do not have internet access or private network, set the traceable IP to that of the upper layer device.



3.4 Virtual Tunnel

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The Gateway supports such VPN protocols as OpenVPN, L2TP, PPTP, and IPsec.

3.4.1 OpenVPN Server

Basic and advanced settings for OpenVPN server are accessible on this page.

Follow the steps below to build an OpenVPN Server:

1. Synchronize the Gateway time with the browser (local) time;
2. Enable the server;
3. Select a protocol;
 TCP provides an ordered delivery of data from user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.
4. Select a working mode between **tap** and **tun**;
 **Tap** bridges two ethernet segments at different locations, so use **tap** if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use **tun**.
5. Assign an input port (leave it as is);
6. Choose the IP address of the WAN port from the drop-down list;
7. Enter the client network IP (leave it as is);

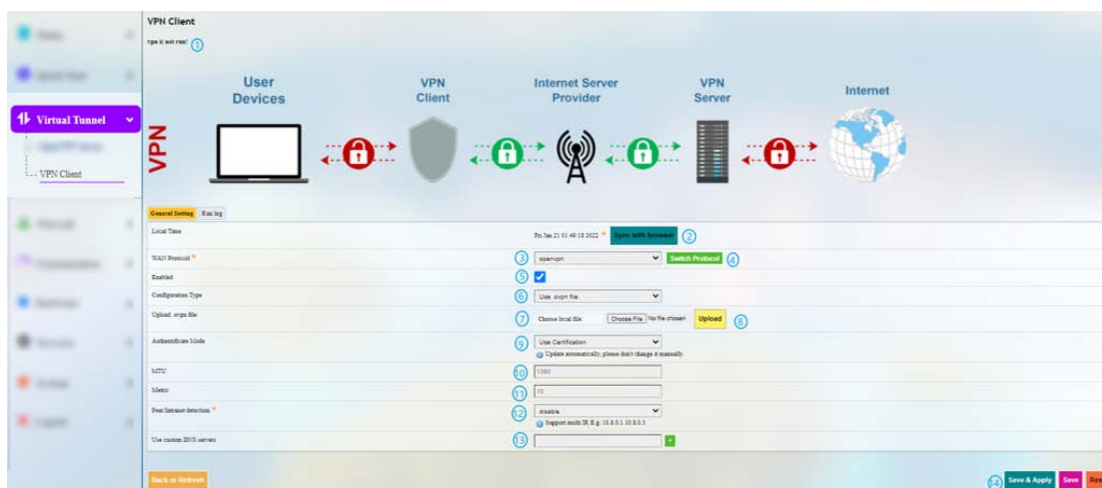
8. Enter the extension configuration (leave it as is);
9. Save the above settings;
10. Download the .ovpn file after applying the settings for further use;
11. When the configurations finish, the status will change as follows.

```
OpenVPN Server  
openvpn server is running---,the pid number: 23162  
CA is ready
```

3.4.2 VPN Client

To configure a VPN client on the Gateway, navigate to **Virtual Tunnel > VPN Client** for specific settings to ensure data confidentiality and undisturbedness.

Before enabling the VPN client, please update the time zone of the client with that of the browser, and complete a time synchronization.



Description of the numbered areas

1. Status of the VPN


▶ If you haven't installed a VPN, there will not be any detailed information.

2. Synchronize your VPN time with the browser (local) time
3. Select a WAN protocol for the virtual line
4. Click to switch to the protocol
5. Check or uncheck the box to enable/disable the protocol


▶ Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to which one you have selected as WAN protocol.

6. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file
7. Select the local .ovpn file for configuration

8. Upload the local profile
9. Select to use a certification or username & password as for authentication
10. MTU settings
11. Metric settings

 The smaller the number, the higher the priority.

12. Disable/Enable heartbeat detection


 Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.

13. Enter custom DNS Servers

14. **Save & Apply** the settings

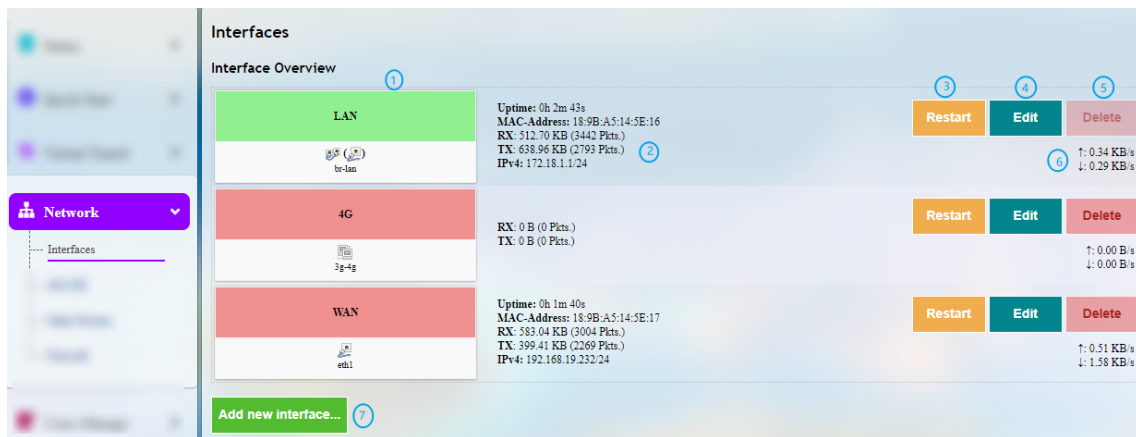
3.5 Network

Despite the fact that the **Network Guide** page under **Quick Start** tab provides access to quick settings of the network, you can check the detailed information of the networks under **Network** tab and make changes accordingly.

 The settings will be overridden if you make changes in the **Network Guide** page under **Quick Start** tab later.

3.5.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces**.



Description of the numbered areas

1. Interface overview
2. Interface details
3. Restart the interface manually
4. Edit the interface settings
5. Delete the interface (available only when you log in as a root user)
6. Instantaneous traffic of the interface
7. Add a new interface (available only when you log in as a root user)

The interfaces will be described in detail in the following sections.

LAN

Upon a click on the **Edit** button behind **LAN**, you'll be directed to the **General Setup** page by default.

The screenshot shows the 'Interfaces - LAN' configuration page. At the top, there is a description of the page and a note about VLAN notation. Below this is the 'Common Configuration' section with two tabs: 'General Setup' (selected) and 'Advanced Settings'. The 'General Setup' tab contains several fields: 'Status' (with a tooltip showing device details like 'Device: br-lan', 'Uptime: 24h 4m 10s', 'MAC: 7d...', 'RX: 164.29 MB (862113 Pkts.)', 'TX: 1.08 GB (1086694 Pkts.)', and 'IPv4: 172.18.1.1'), 'Protocol' (set to 'Static address'), 'IPv4 address' (set to '172.18.1.1'), and 'IPv4 netmask' (set to '255.255.255.0'). Numbered callouts 1, 2, and 3 point to the Status field, the IPv4 address field, and the IPv4 netmask field respectively.

Description of the numbered areas

1. Status of the interface
2. IP address of the LAN interface
3. Select a LAN interface subnet mask

In the common configuration area, click **Advanced Settings**:

The screenshot shows the 'Interfaces - LAN' configuration page, specifically the 'Advanced Settings' tab. It contains three fields: 'Override MAC address' (set to '7d:d1:b8'), 'Override MTU' (set to '1500'), and 'Use gateway metric' (set to 'Same as 'Auto Routing''). Numbered callouts 1, 2, and 3 point to the Override MAC address field, the Override MTU field, and the Use gateway metric field respectively.

Description of the numbered areas

1. MAC address cloning
2. MTU settings
3. Keep the metric same as Auto Routing or customize the metric

▶ Be sure to save the settings before you exit the page.

When you log in to VantronOS as a root user (**password: rootpassword**), there will be a **Physical Settings** tab next to **Advanced settings**, which allows you to configure the LAN port for network bridge.

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup | Advanced Settings | **Physical Settings**

Bridge interfaces 1 ☒ creates a bridge over specified interface(s)

Enable STP 2 ☐ Enables the Spanning Tree Protocol on this bridge

Interface 3

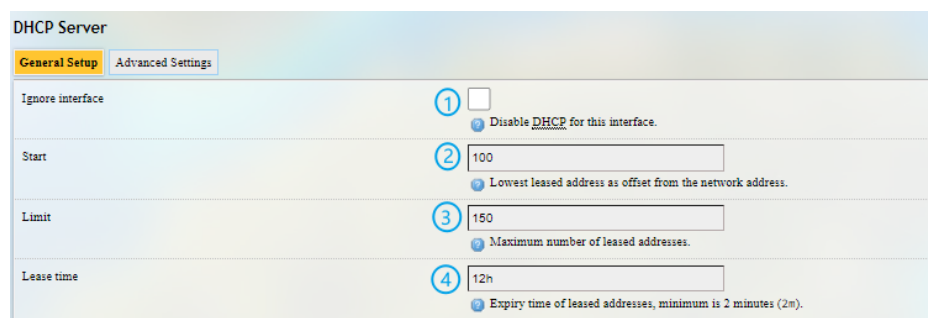
- ☐ Ethernet Adapter: "can0"
- ☐ Ethernet Adapter: "erspan0"
- ☒ Ethernet Adapter: "eth0" ([lan](#))
- ☐ Ethernet Adapter: "eth1" ([wan](#))
- ☐ Custom Interface:

Description of the numbered areas

1. Enable the interface for network bridge
2. Enable STP protocol
3. Select the interface for bridge connection

LAN – DHCP

In the **General Setup** page of DHCP Server under **Common Configuration** of LAN port, DHCP could be set up with more details:



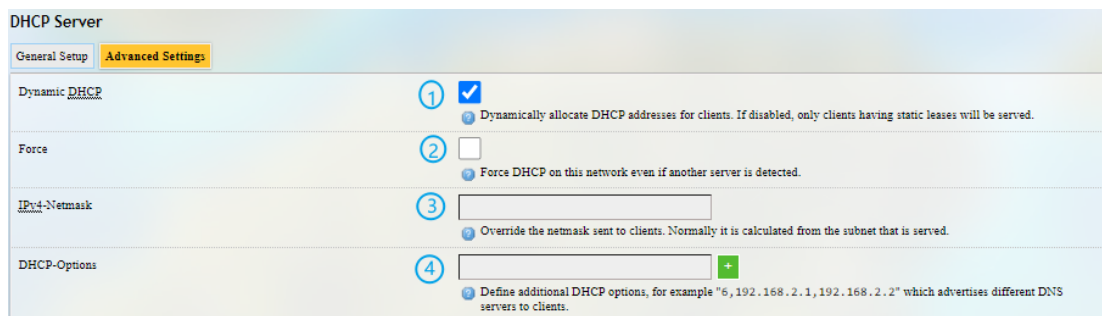
Description of the numbered areas

1. Disable DHCP service

 If disabled, DHCP service will not take effect to this interface.

2. DHCP start address
3. Maximum number of leased addresses (up to 150)
4. Expiry time of leased addresses (min. 2m)

Advanced Settings of DHCP Server:



Description of the numbered areas


1. Enable dynamic allocation of addresses for clients

 If disabled, clients shall have static leases.

2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

 Normally it is calculated from the subnet that is served

4. Add different DNS servers for clients

 Be sure to save the settings before you exit the page. Clicking on Back or Refresh will get you back to interface settings.

4G

You'll be redirected to 4G/LTE configuration page upon a click of the **Edit** button behind 4G interface. Refer to [3.5.3 4G/LTE](#) for details.

WAN

General and advanced settings of WAN interface are configured here.

WAN – DHCP Client

General DHCP protocol settings for WAN interface are shown below.

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g., eth0.1).

Common Configuration

General Setup | Advanced Settings

Status	1	Device: eth0.2 Uptime: 22h 5m 9s MAC: 8E:D9:97:00:00:02 RX: 929.56 MB (1193522 Pkts.) TX: 135.71 MB (645207 Pkts.) IPv4: 192.168.1.1
Protocol	2	DHCP client
Hostname to send when requesting DHCP	3	VantronOS-B4A7

Description of the numbered areas

1. Status of the WAN port
2. Select DHCP client as WAN protocol or switch to another protocol
3. Hostname to send when requesting DHCP

Advanced DHCP protocol settings for WAN interface are shown below.

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g., eth0.1).

Common Configuration

General Setup | **Advanced Settings**

Use default gateway	1	<input checked="" type="checkbox"/> If unchecked, no default route is configured
Use DNS servers advertised by peer	2	<input checked="" type="checkbox"/> If unchecked, the advertised DNS server addresses are ignored
Use gateway metric	3	Same as 'Auto Routing'
Override MAC address	4	8E:D9:97
Override MTU	5	1500

Description of the numbered areas

1. Enable **Use default gateway**
2. Enable **Use DNS server advertised by peer**
3. Gateway metric
4. MAC address cloning
5. Network MTU



Be sure to save the settings before you exit the page.

WAN – Static Address

To activate static address protocol, select **Static address** in the drop-down list as the protocol and click **Switch protocol**.

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup

Status

Device: eth1
Uptime: 1h 40m 27s
MAC: 18:9...
RX: 154.48 MB (212045 Pkts.)
TX: 95.86 MB (177212 Pkts.)
IPv4: 192...

Protocol: Static address

Really switch protocol?

Switch protocol

Upon click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast. Custom DNS server could also be added.

- ▶ Leave the field as is if not available.
- ▶ When static address protocol is selected, DHCP server will be automatically disabled.
- ▶ The advanced settings are basically same as those for DHCP protocol.

WAN – PPPoE

The general and advanced PPPoE settings for the WAN port are literally the same as those above. Clicking on **Back or Refresh** will get you back to interface settings.

3.5.2 Wireless (WIFI)

You can switch between AP and client modes for wireless connection.

Wi-Fi – AP Mode (General settings)

The screenshot displays the 'Wi-Fi Settings' page for an AP mode. It includes a 'General Setting' tab and an 'Advanced Setting' tab. The 'General Setting' tab contains the following fields:

- Status: Mode: Master / SSID: Vantron-2B8892, BSSID: 0C:CF:89:2B:88:92, Encryption: mixed WPA/WPA2 PSK (CCMP), Channel: 1 (2412 GHz), Tx-Power: 20 dBm, Signal: -37 dBm, Noise: -95 dBm, Bitrate: 300.0 Mbit/s, Country: US
- WiFi mode: AP (with a 'Switch Mode' button)
- SSID: Vantron-2B8892 (marked with a blue circle 1)
- Channel: 1(2412MHz) (marked with a blue circle 2)
- Encryption: WPA-PSK/WPA2-PSK Mixed Mode (marked with a blue circle 3)
- Cipher: Force CCMP (AES) (marked with a blue circle 4)
- Key: ***** (marked with a blue circle 5)

Below the settings is an 'Associated Stations' table:

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
(Master: "Vantron-2B8892") (marked with a blue circle 6)	D6:A2:A0:00:00:00	172.1	-37 / -95 dBm	65.0 Mbit/s, 0Mhz 65.0 Mbit/s, 0Mhz

At the bottom, there are buttons for 'Back or Refresh', 'Save & Apply', 'Save', and 'Reset'.

Description of the numbered areas

1. Set an SSID for the Gateway

 The ID name shall not contain characters including \$, `, \.

2. Select a Wi-Fi channel

3. Select an encryption method (the following options vary with the encryption method)

4. Select an encryption algorithm

5. Assign a Wi-Fi password (no less than 8 characters)

6. List of currently connected devices

Wi-Fi – AP Mode (Advanced setting)

WIFI Settings

General Setting **Advanced Setting**

Enable/Disable WIFI ① **Disable WIFI**

WIFI Frequency ② 2.4G **Switch Frequency** ③

Band ④ HT40

Note: select HT option for 80211n mode.

Transmit Power ⑤ auto

dBm

Network ⑥ ☒ lan ☐ wds

Choose the network(s) you want to attach to this wireless interface

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
(Station: "Vantron-2B8892")	D6-A2-A1	172.1	-37 / -95 dBm	72.0 Mbits, 0MHz 72.0 Mbits, 0MHz

Description of the numbered areas

1. Turn on/off Wi-Fi
2. Set Wi-Fi frequency (determined by hardware)
3. Click to switch frequency
4. Set Wi-Fi band
5. Wi-Fi transmission power
- ▶ Fields 2-5 will depend on the functions of the Wi-Fi module, for example, RTL8188 wireless module does not have such options.
6. The network interface to which Wi-Fi belongs

Wi-Fi – Client Mode

When the Gateway is set as a client on a wireless network, the page below allows you to make changes to the network settings.

▶ The parameters will be overwritten if you change the settings under [3.3.3 WAN Setting – Client](#).

▶ A wwan0 port will be added automatically when client mode is being configured.

Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically get an IP or Static Address protocol to specify an IP for the Gateway
3. Select a wireless network for internet access
4. Click **Scan WIFI** to refresh the Wi-Fi list if the target Wi-Fi is not identified
5. Select the MAC address of the Wi-Fi, or leave it to Auto if not clear
6. Input the password of the Wi-Fi
7. Confirm that the target Wi-Fi has internet connection

When the Gateway is successfully connected as a client, there will be the network information next to **Scan WIFI** button.

3.5.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card in the slot.

Confirm with your sales representative whether the 4G module is AT&T or Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCI-E-4G**.

Remember to ask the carriers for the APN which needs to be filled in the system during 4G setup.

If you have inserted an activated SIM card in the slot, the SIM card information will display on the top of the page, including signal strength, IP, and IMEI. While register status, device node, SIM card ICCID and other general information will display at the bottom of the page.

The screenshot displays the '4G/LTE' configuration page. At the top, it shows 'SIM Card: READY', 'Sig: 94%', 'GET IP: 10.211.150.186', and 'IMEI: 86022...'. Below this are tabs for 'General Setting' (selected), 'Advanced Setting', 'Run log', and '4G traffic'. A circled '6' is next to the 'Advanced Setting' tab. The 'General Setting' section includes a 'Status' field, an 'Enable/Disable' dropdown set to 'enable' (marked with a circled '1'), a 'Dial number' field with '*99***1#' (marked with a circled '2'), an 'APN' field with '3gnet' (marked with a circled '3'), a 'PAP/CHAP username' field with 'your_username' (marked with a circled '4'), and a 'PAP/CHAP password' field with masked characters (marked with a circled '5'). To the right of these fields is a 'Device' info box showing '3g-4g', 'Uptime: 1h 47m 10s', 'RX: 252.01 KB (2354 Pkts.)', 'TX: 201.70 KB (2163 Pkts.)', and 'IPv4: 10.211.150.186/32'. The 'General Information' section at the bottom lists: 'SIM Slot 1: Inserted', 'SIM Slot 2: Not Detected', 'SIM is using: SIM 1', 'Register Status: Registered', 'Device node: Pre-certified modem on /dev/ttyACM0', 'Register Type: LTE', 'SimCard IMSI: 460018972603921', 'SimCard ICCID: 8...03', and 'Modem Firmware: CAT1.LE910-NA1.VT-XOS V2.10.20.00.525'.

Description of the numbered areas

1. Enable/disable 4G/LTE service
2. Input *99***1# for AT&T SIM card and *99***3# for Verizon SIM card
3. Input the APN provided by the carrier
4. Enter the username provided by the carrier for PAP/CHAP authentication
5. Enter the password provided by the carrier for PAP/CHAP authentication
6. Click **Advanced Setting** for more configuration options

- ▶ Leave the field as is if not available.
- ▶ PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

In the **Advanced Setting** page, you can further configure the cellular network.

4G/LTE

SIM Card: READY Sig: 94% GET IP: 10.211.150.186 IMEI: 8602...

General Setting **Advanced Setting** Run log 4G traffic

SIM card switching ① 2
② When SIM dialing fails the preset number of times, switch to another SIM card

Restart Module ② **Re-power**

Auto Re-power Module ③ 5 min
④ Re-power the module, when the internet connection is offline more than preset time

PDP Type ④ ALL
⑤ PDP Type: ALL or IPV4_Only or IPV6_Only

CID Value ⑤ 1
⑥ CID, default: 1

Provider ⑥ AT&T/TMO/Canada

Override MTU ⑦ 1500

General Information

SIM Slot 1:	Inserted
SIM Slot 2:	Not Detected
SIM is using:	SIM 1
Register Status:	Registered
Device node:	Pre-certified modem on /dev/ttyACM0
Register Type:	LTE
SimCard IMSI:	460018972603921
SimCard ICCID:	8 003
Modem Firmware:	CAT1,LE910-NA1,VT-XOS_V2.10.20.00.525

Description of the numbered areas

1. Maximum number of dial failures allowed for current SIM card (available only for devices with dual SIM cards, leave it as is)
2. Click to restart the 4G module
3. Time scheduled for automatic restart of the 4G module when it is offline
4. Select a PDP type (leave it as is)
5. Select **custom** from the drop-down list, input 1 for AT&T SIM card and 3 for Verizon SIM card
6. Select **AT&T/TMO/Canada** or **Verizon** from the drop-down list for AT&T SIM card and Verizon SIM card, respectively
7. Default MTU value (1500)

- ▶ Remember to save the settings to have the configurations take effect.

If your 4G module is not AT&T and Verizon pre-certified, the provider information will not be available in **Advanced Setting**, and the **General Setting** options are the same as those for pre-certified 4G module. You can keep the default values of the fields unchanged.

4G/LTE

SIM Card: READY Sig: 94% GET IP: 10.211.150.186 IMEI: 86021

General Setting Advanced Setting Run log 4G traffic

SIM card switching	<input type="text" value="2"/> <small>When SIM dialing fails the preset number of times, switch to another SIM card</small>
Restart Module	Re-power
Auto Re-power Module	<input type="text" value="5 min"/> <small>Re-power the module, when the internet connection is offline more than preset time</small>
PDP Type	<input type="text" value="ALL"/> <small>PDP Type: ALL or IPV4_Only or IPV6_Only</small>
CID Value	<input type="text" value="1"/> <small>CID, default: 1</small>
Override MTU	<input type="text" value="1500"/>

General Information

SIM Slot 1:	Inserted
SIM Slot 2:	Not Detected
SIM is using:	SIM 1
Register Status:	Not registered, not currently searching a new operator to register to
Device node:	EC200T LTE modem on /dev/ttyUSB2
Register Type:	Unkown
SimCard IMSI:	loading---
SimCard ICCID:	loading---
Modem Firmware:	EC200T,EC200TCNDAR02A15M16

The **Run Log** next to the **Advanced Setting** tab provides the last 50 log entries of the module.

Under **4G traffic** tab, information about real-time traffic, monthly traffic, and daily traffic is available.

3.5.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Example:

Requirement: When the Gateway has 4G and WAN network interfaces, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN interface by the internal server. Other data access is realized via the 4G interface.

Click **Add** and select an interface to configure.

Routes
Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target <small>Host-IP or Network</small>	IPv4-Netmask <small>if target is a network</small>	IPv4-Gateway	Metric	MTU	Route type	
wan	192.168.0.0/16	255.255.255.255	192.168.9.222	0	1500	unicast	Delete

Add **Save & Add** **Reset**

Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.5.5 Firewall

Firewall – General Settings

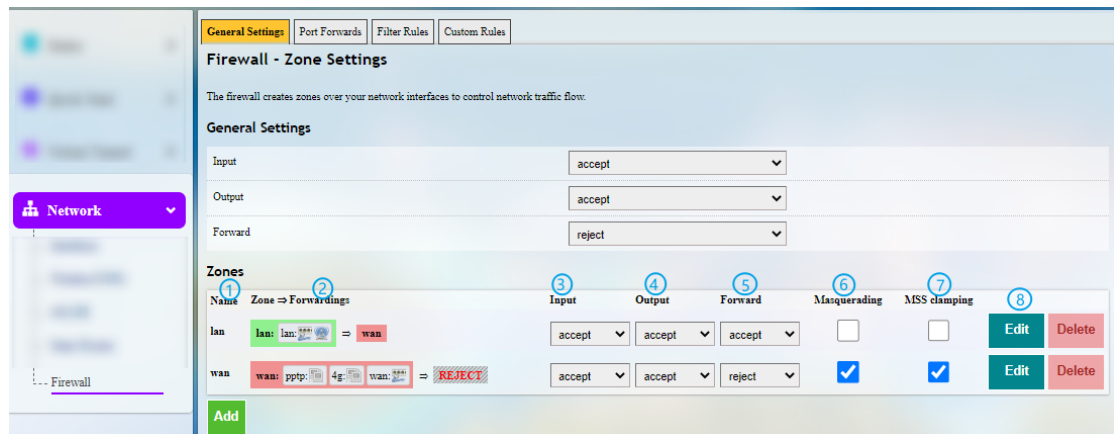
The following is a summary of the configuration items that the firewall can define. The minimum firewall configurations usually contain a basic setting item, at least two zones (LAN and WAN) and a forwarding to allow packets to be forwarded from LAN to WAN.

General Settings define the global settings that do not depend on a specific area. The following options can be defined:

Name	Type	Mandatory or not	Default value	Description
Input	String	N	ACCEPT	INPUT chain default strategy (ACCEPT, REJECT, DROP)
Forward	String	N	REJECT	FORWARD chain default strategy (ACCEPT, REJECT, DROP)
Output	String	N	ACCEPT	OUTPUT chain default strategy (ACCEPT, REJECT, DROP)

Firewall – Zone Settings

A zone section groups multiple interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis.



Description of the numbered areas

1. Unique zone name

▶ At least LAN and WAN shall be listed under the zone name.

2. Zone forwarding model description

3. Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic

4. Default policy (ACCEPT, REJECT, DROP) for outgoing zone traffic

5. Default policy (ACCEPT, REJECT, DROP) for forwarded zone traffic

6. Masquerading (NAT)

7. MSS clamping

8. Zone editing

A click of the **Edit** button following each zone will direct you to the detailed zone setting page where general settings, advanced settings and forwarding rules are available.

Firewall – Port Forwards

The forwarding sections control the traffic flow between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwardings are required, with src and dest reversed in each.

Illustrative example on port forwarding (Forwarding port 3222 (WAN) to port 22 of LAN host 172.18.1.174):

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Name	Match	Forward to	Enable				
3222to22	IPv4-tcp, udp From any host in wan Via any router IP at port 3222	IP 172.18.1.1, port 3222 in lan	<input checked="" type="checkbox"/>	Up	Down	Edit	Delete

New port forward

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
3222to22	TCP+UDP	wan	3222	lan	172.18.1.174 (WIM-20210305RYJ.la)	22	Add

Description of the numbered areas

1. Rule name
2. Protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: LAN
6. LAN host: 172.18.1.174
7. Target host port number of the internal zone: 22
8. Add rules (mandatory)

Firewall – Custom Rules

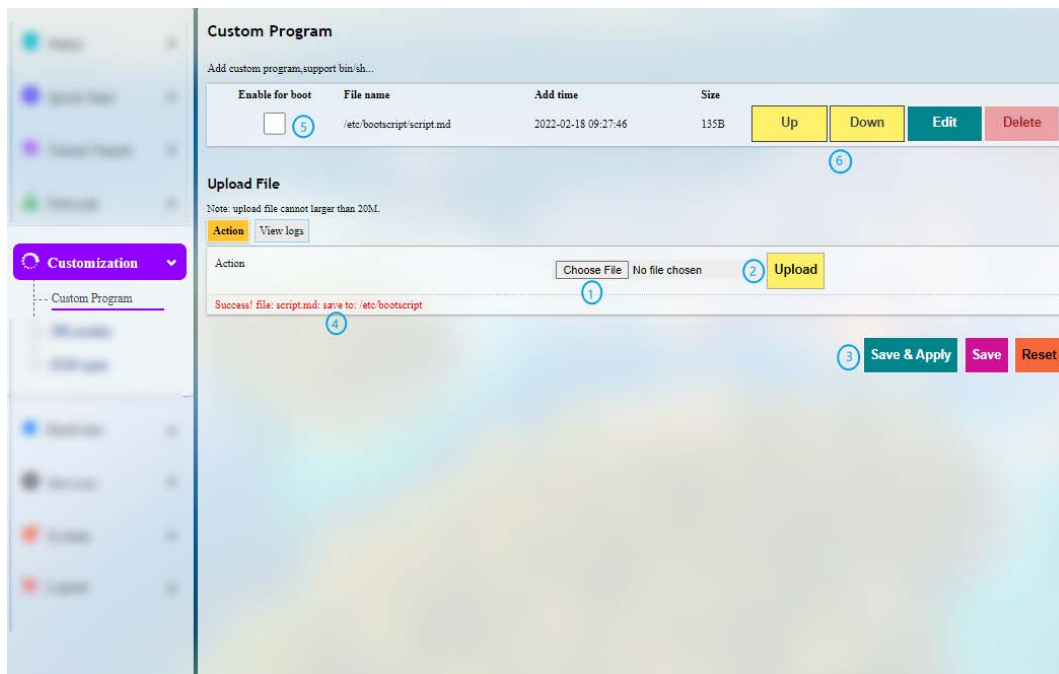
Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.

3.6 Customization

Customization is supported depending on the device model. For some devices other than G202, this function may not be available.

3.6.1 Custom Program

Custom program allows users to upload scripts or programs (sh/bin) to the Gateway and run them at the startup.



Description of the numbered areas

1. Select a script to upload
2. Upload the script to the Gateway
3. **Save & Apply** the settings
4. When the script is uploaded successfully, the file name and file directory will be displayed
5. Enable the script, and it will run next time when the Gateway starts up
6. If more than one script is uploaded, you can move any of them up or down to rearrange the script order, and edit/delete the script

3.6.2 IPK Installer

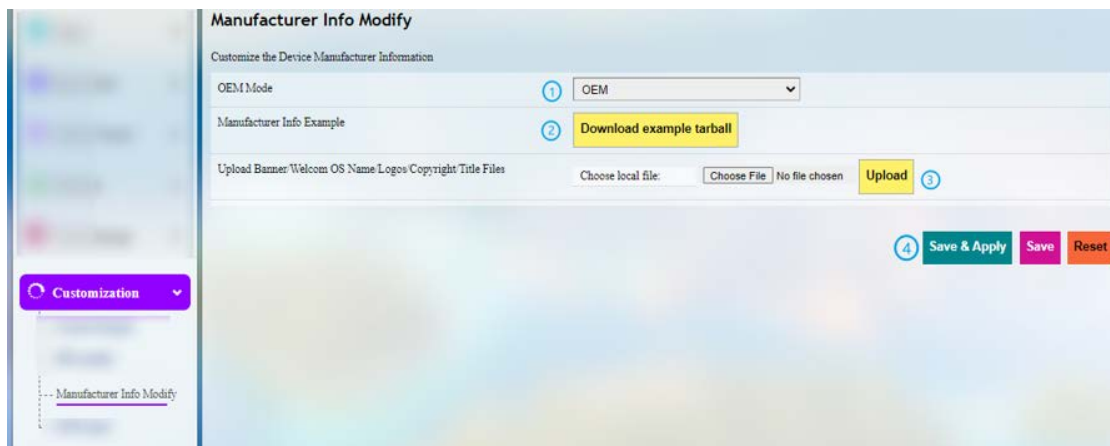
With IPK Installer, customers can install self-compiled IPK packages to the Gateway. Vantron industrial protocol packages are also uploaded from here. Refer to [4.2 Protocol Configuration and Application](#) for Industrial Protocols.

3.6.3 Manufacturer Info Customization

As modifications made to this function will change system information, it is required that users log in to the system with **root** account and password as indicated in [2.2 Gateway Login](#).

- Account: root
- Password: rootpassword

Once you need to customize the manufacturer information, navigate to **Customization > Manufacturer Info Modify**, and select OEM from the **OEM Mode** drop-down list.



Description of the numbered areas

1. Select OEM mode
2. Download illustrative tarball
3. Replace the files in the package as needed and upload the file one by one
4. **Save & Apply** the settings

There are three modes that customers can choose from the drop-down list based on their needs.

Vantron: All the information included in the files will be about Vantron.

Standard: Some of the fields included in the files will be “Gateway” by default, and some information like the copyright will be left blank.

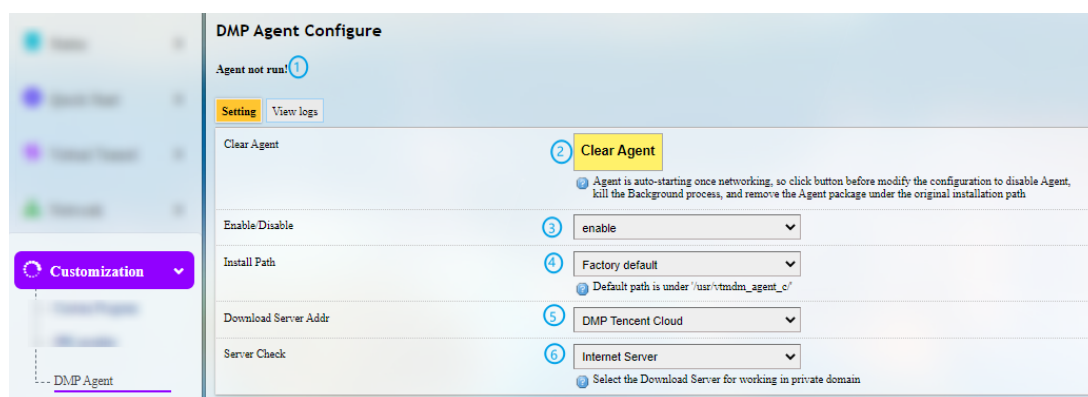
OEM: All the information displayed will be user tailored.

3.6.4 DMP Agent

DMP Agent is designed for communication with Vantron gateway management platform, a console where multiple gateways could be managed in groups to provide required information of a target workplace. With the platform, devices connected to each gateway will be displayed with detailed information, including variables, data collection status, edge computing information, etc.

If you are provided with a token for the Gateway, you just need copy the Gateway SN (on the Status page) to the platform to track all the devices connected to it.

More information will be available in the user manual of the gateway management platform.



Description of the numbered areas

1. Status of DMP Agent
2. Click **Clear Agent** before changing the configurations

▶ DMP Agent runs automatically once there is internet access. Clicking this button will disable DMP Agent, kill all the processes running at the background, and remove the Agent package in the original installation directory.

3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here

▶ The Agent is installed in “/usr” by default. The available space of G202 is 13MB not enough for the Agent, so it is recommended that the directory is mounted to /mnt/sda1, the mounting directory of the Micro SD card. Therefore, remember to format the SD card to ext4 file system and install the SD card before configuration.

5. Set up the download address of the Agent server (suggest not changing the address)
6. Check the server

You'll be able to manage the Gateway on your portal.

3.7 Hardware

3.7.1 Ser2TCP

Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.



When clicking **Edit** behind a device, you'll be able to make advanced settings. Under the server mode, three protocols are available which are differentiated as below:

A screenshot of the 'Advanced Setting' interface for the Ser2TCP device. The interface has a sidebar on the left with a 'Hardware' section expanded, showing 'Ser2TCP' selected. The main area contains the following settings:

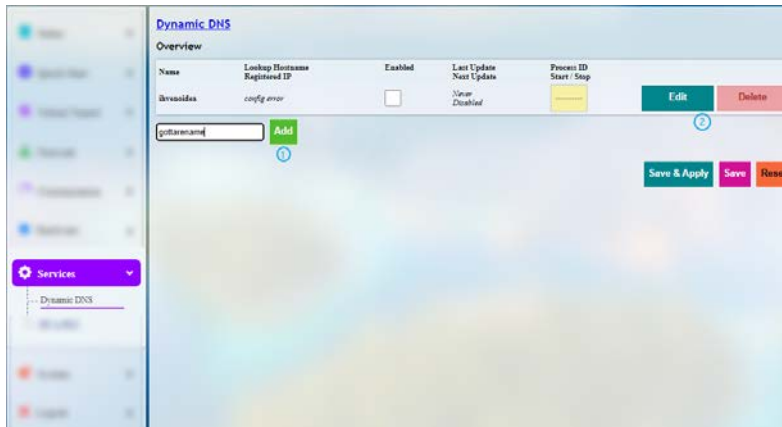
Advanced Setting	
Enable/Disable	Disable
Work mode	Work as server
Port	5000
Protocol	Telnet
Device	/dev/ttyS0
Baud Rate	115200
Timeout	0
Data Bits	8 bits
Parity	None
Stop Bits	1

- 1) Raw: enables the port and transfers all data as-is between the port and the long.
- 2) Rawlp: enables the port and transfers all input data to a gateway that is open without any Termios settings, allowing to use /dev/lpx devices and printers connected.
- 3) Telnet: enables the port and runs the telnet protocol on the port to set up telnet parameters (less used).

3.8 Services

3.8.1 Dynamic DNS

Dynamic DNS is a technology in domain name system (DNS) that automatically updates the content of the Name Server, often in real time, with the activated DDNS configuration of its configured hostnames, addresses or other information.



Description of the numbered areas

1. Enter the name of the subdomain or root domain and click **Add** button, you will be directed to the setup page of the dynamic DNS. Then you can enter username, password, the hostname/domain you created, etc.;
2. For a created subdomain or root domain, you can enable/edit/delete it here.

3.8.2 RC to PLC

For remote access and control of the PLCs via OpenVPN protocol, you need configure a .ovpn file and upload it to the gateway then restart the core process to activate remote connection. Once ready, configure the IP address of the PLC and save the settings to apply.

The screenshot shows a web interface titled "Remote connect to PLC". It is divided into two main sections: "Step 1: Upload key" and "Step 2: Configure IP mapping".

Step 1: Upload key

At the top, there are two tabs: "General Setting" (active) and "Run log". Below the tabs, the text "Upload plc2down key file" is displayed. To the right of this text is a "Choose File" button (labeled 1) and a "No file chosen" label. Further right is a yellow "Connect" button (labeled 2). Below the "Connect" button, a green "Restart core" button is visible, followed by the text "Connected, IPAddr: 10.8.0.2" (labeled 3).

Step 2: Configure IP mapping

This section contains a table with the following columns: "status", "plc ip addr", "virtual ip", and "Remarks".

status	plc ip addr	virtual ip	Remarks
ready	172.18.1.132 (labeled 4)	10.8.0.6 (labeled 5)	

Below the table, there is a green "Add" button on the left and a red "Delete" button on the right.

Description of the numbered areas

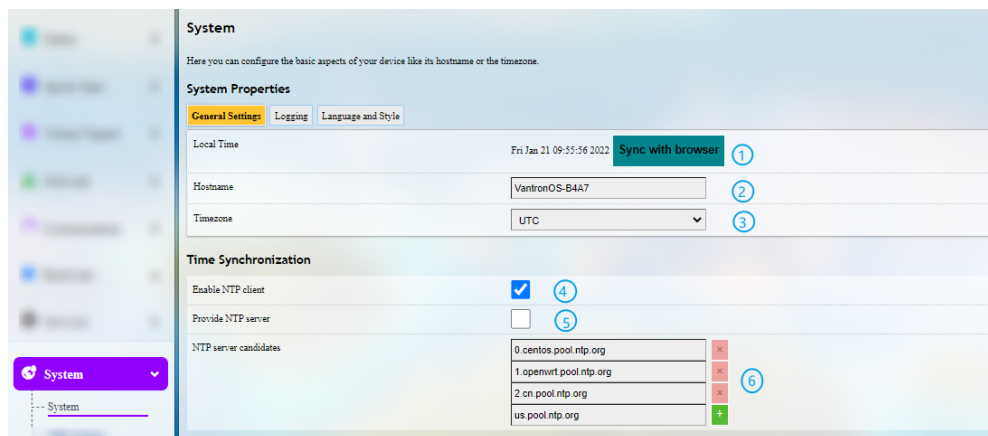
1. Locate the .ovpn file downloaded as per [3.4.1 OpenVPN Server](#)
2. Click **Connect** to upload the file
3. After connection, an IP address assigned by OpenVPN server will be displayed here
4. Input the IP address of the PLC (on the same network subnet as the Gateway LAN port)
5. Input the virtual IP (on the same network subnet as the one assigned by OpenVPN server)

After finishing above configurations, you'll need to install and run OpenVPN client on the PC, then connect the running PLCs with the client to control the PLCs remotely. The communication interface could be edited in **Interfaces** under **Network** Tab.

3.9 System

Apart from the device settings you might make in the previous sections, here you can configure your Gateway in more details, including host name, time zone, administrative password and so on.

3.9.1 System



Description of the numbered areas

1. Synchronize the Gateway time with the browser (local) time
2. Assign a name to the host
3. Select a time zone
4. Enable NTP online time adjustment
5. Start the NTP server (the Gateway)
6. NTP online time server

For log-related settings, click **Logging** tab next to the **General settings** tab. If you want to change the interface language, just navigate to **Language and Style** tab following behind.

3.9.2 NBM Setting

General Settings

Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

General Settings | Advanced Settings | Protocol Mapping

Accounting period 1
 Choose "Day of month" to restart the accounting period monthly on a specific date, e.g. every 3rd. Choose "Fixed interval" to restart the accounting period exactly every N days, beginning at a given date.

Due date 2
 Day of month to restart the accounting period. Use negative values to count towards the end of month, e.g. "-5" to specify the 27th of July or the 24th of February.

Local interfaces 3 ☒ lan ☐ ppp ☐ wan
 Only comtrack streams from or to any of these networks are counted.

Local subnets 4
 Only comtrack streams from or to any of these subnets are counted.

Description of the numbered areas

1. Set how long you would like the monitoring activities to be summarized
2. Specify a day in month for restarting another round of monitoring activities
- ▶ Applicable when Day of month is selected in 1
3. Statistics interface
4. Local subnets

Under **Advanced Settings** tab, each setting item is explained in detail so that users can figure out how to configure accordingly.

Protocol Mapping can be used to distinguish traffic types per host. Each mapping takes one line, with the first value being the IP protocol, the second value being the port number, and the third value being the name of the mapping protocol.

3.9.3 Administration

Under **Router Password** section, you can reset a password for accessing the Gateway.

SSH Access

As this function might compromise the security of the network, you have to log in the web interface with a root account.

Step 1: Log out the interface by clicking **Logout** at the left bottom corner;

Step 2: Log in with the account and password provided in [2.2 Gateway Login](#);


Account: root

Password: rootpassword

Step 3: Navigate to **System > Administration**, and enable dropbear.

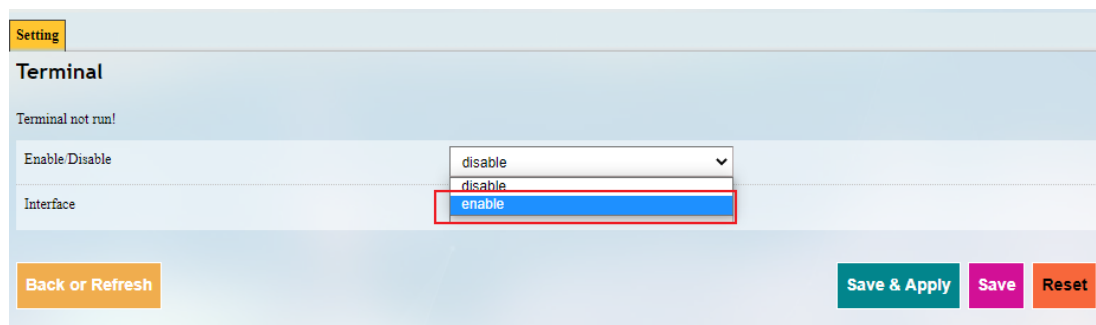


Description of the numbered areas

1. Select a port to access (LAN by default)
 When “unspecified” is selected, all the ports will be monitored.
2. Specify a port for monitoring (port 22 by default)
3. Allow SSH password authentication
4. Add SSH-Keys for public key authentication

3.9.4 Terminal

When the web terminal is enabled, you can log in and input command lines here.



Setting

Terminal

Terminal not run!

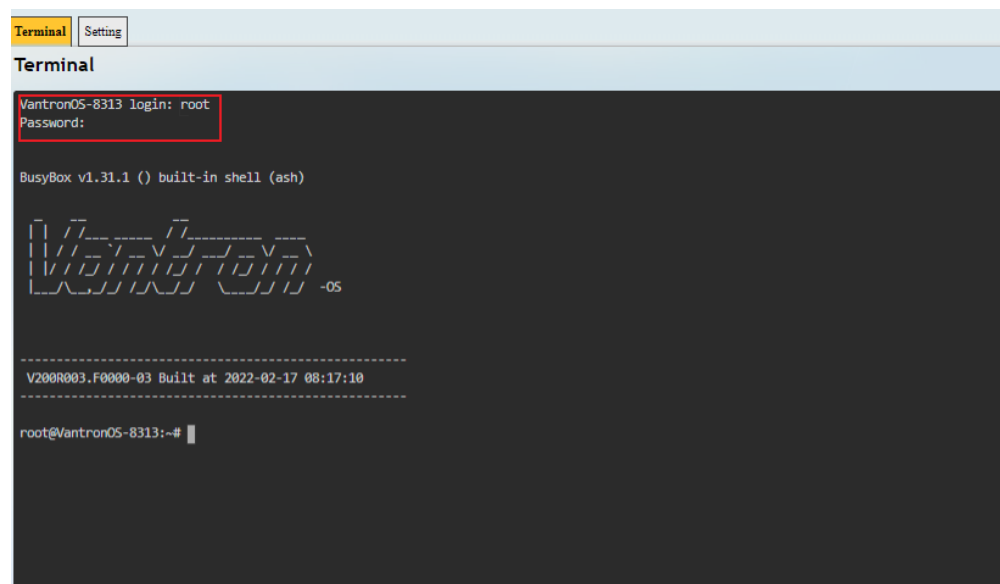
Enable/Disable: disable

Interface: enable

Back or Refresh Save & Apply Save Reset

Login name: root

Login password: rootpassword (invisible while typing)



Terminal Setting

Terminal

VantronOS-8313 login: root

Password:

BusyBox v1.31.1 () built-in shell (ash)

VantronOS

V200R003.F0000-03 Built at 2022-02-17 08:17:10

root@VantronOS-8313:~#

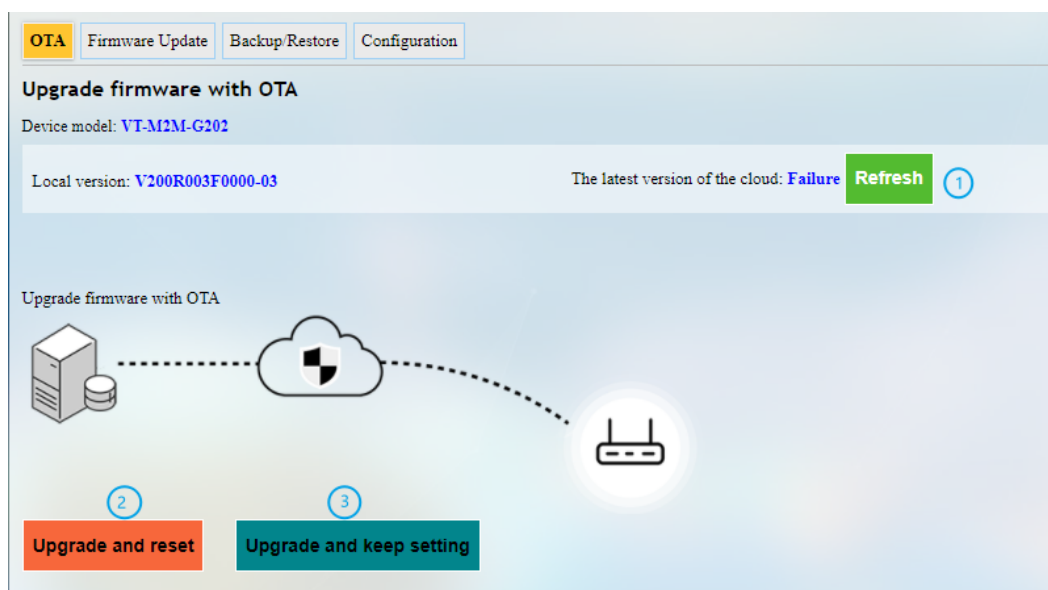
3.9.5 Mount Points

You can enable/disable automount and check the mounting information here.

3.9.6 Backup/Flash Firmware


On this page, you can backup/restore parameters, restore factory settings (clear user settings), and upgrade the firmware from local or with OTA application.

OTA upgrade



Description of the numbered areas

1. Refresh the cloud version to the latest (internet access required)
2. Upgrade the Gateway and reset to default settings
3. Upgrade the Gateway and keep the existing settings unchanged

 If the cloud version is shown **Failure**, the Gateway is not activated from the cloud, please contact your sales representative for solution.

You can also upload an image under **Firmware Update** tab to replace the old-version firmware while keeping the existing settings unchanged.

Under **Backup/Restore** tab, you can download the backup package of your settings, including configuration files and pre-set folders, restore the factory settings of the Gateway, and upload the backup package saved before.

Under **Configuration** tab, you can customize the configuration files or directories to be retained during the upgrade.

3.9.7 Reboot

Make sure you do not have any ongoing process before rebooting the Gateway.

3.10 Logout

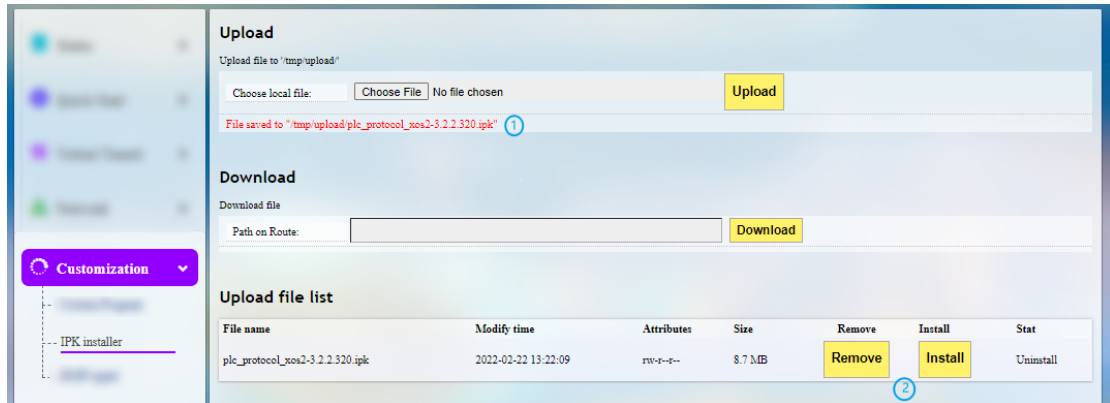
You will exit the web interface with a click on the **Logout** tab. If you need re-log the web, use the default password: **admin**. Make sure you have saved the changes before logout.

CHAPTER 4

INDUSTRIAL PROTOCOL CONFIGURATION

4.1 IPK Installation for Industrial Protocols

In VantronOS web interface, navigate to **Customization > IPK installer**, and upload the .ipk file for industrial protocol configuration.



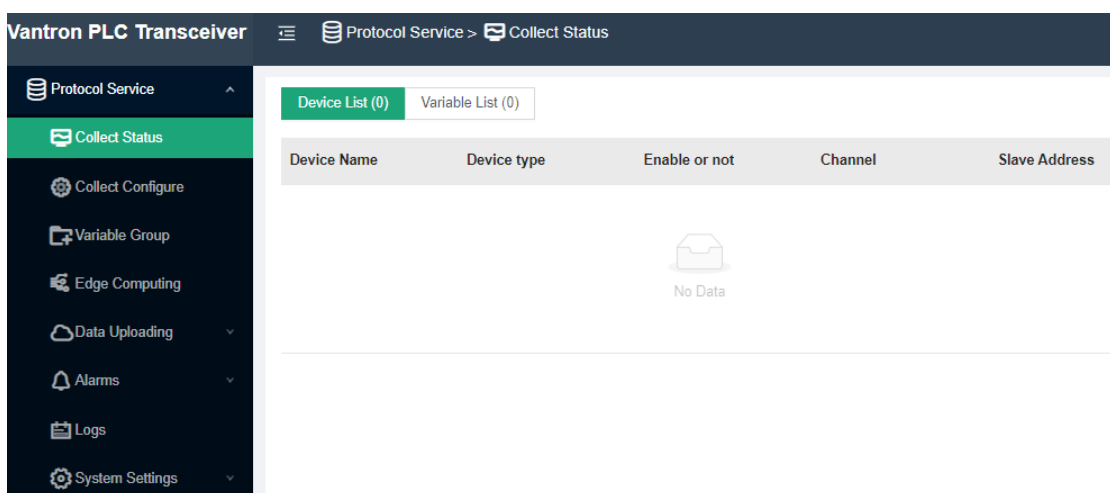
Description of the numbered areas

1. After the .ipk file is uploaded to the Gateway, the directory of the file will be displayed
2. You can remove or install the .ipk thereafter

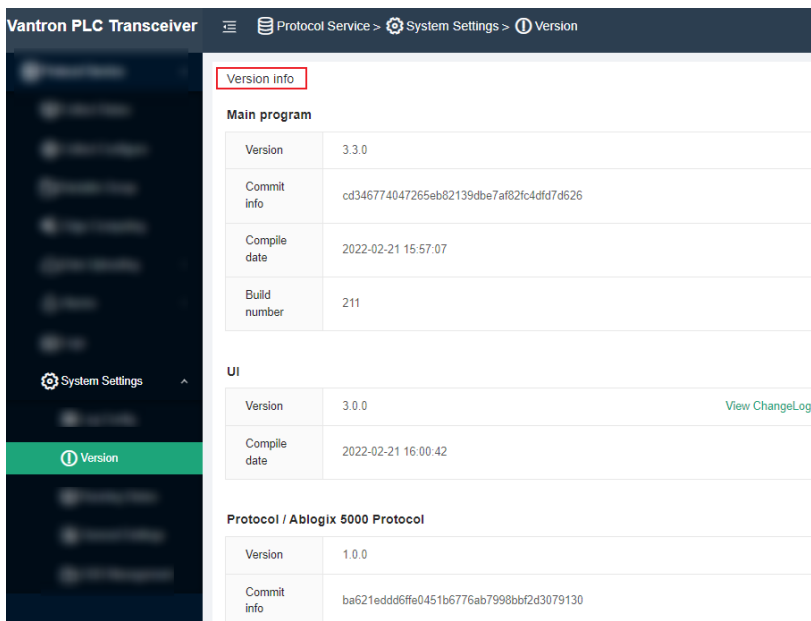
Once the .ipk file is installed, a message will be displayed suggesting the status of the file installation as shown below.



Input the port number (8081) after the Gateway IP in the address bar, for instance: 172.18.1.1:8081, and enter the protocol web interface which looks like below.



You can check the version information of the protocol package under **System Settings**.

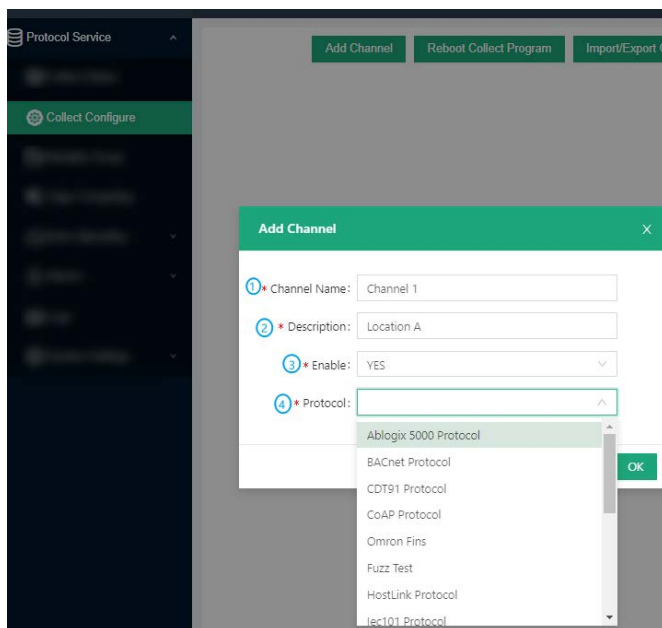


4.2 Protocol Configuration and Application

To use a protocol for data acquisition and edge computing, figure out the device model you are using for data collection and configure the protocol accordingly.

4.2.1 Configuration of Data Acquisition Protocols

Click **Collect Configure** on the left navigation pane to add a channel for data collection.



Description of the numbered areas

1. Enter a channel name that shall not be any one of the names in use
2. Describe the channel
3. To enable the channel or nor (Yes by default)
4. Select a protocol type from the drop-down list based on the type of the data collection device (the protocols are supported by the .ipk file installed)

For certain protocol, more configuration parameters are required. Taking Modbus RTU protocol as an example, further information is needed.

The screenshot shows a configuration window titled "Add Channel" with a close button (X). It contains 12 numbered fields for channel configuration:

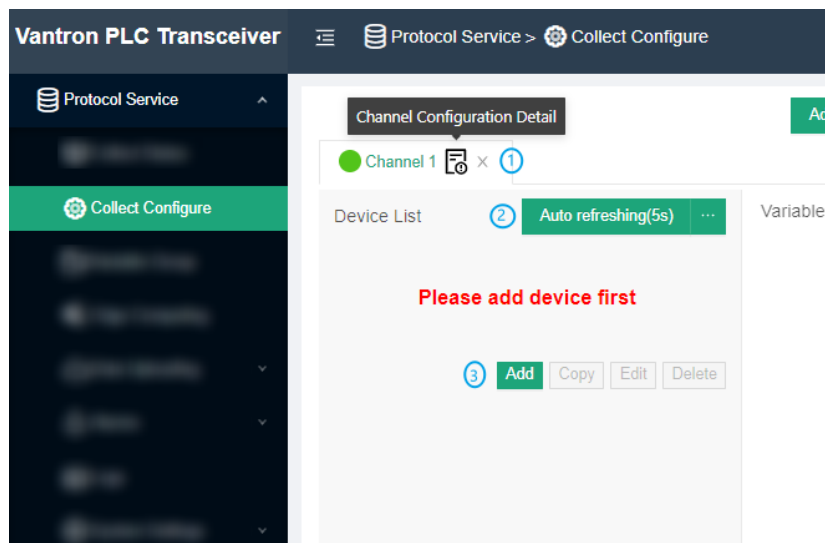
- 1 * Channel Name: Channel 1
- 2 * Description: Location A
- 3 * Enable: YES
- 4 * Protocol: Modbus Protocol
- 5 Communication: modbus serial
- 6 * Protocol Mode: Modbus RTU
- 7 * Serial Port:
- 8 * Serial Mode: RS485
- 9 * Baudrate: 9600
- 10 * Data Bits: 8
- 11 * Parity: N
- 12 * Stop Bits: 1

At the bottom, there are "Cancel" and "OK" buttons.

Description of the numbered areas

4. Select Modbus protocol
5. Choose serial or TCP communication
6. Both Modbus RTU and Modbus ASCII are available (Modbus RTU for example)
7. Select the exact serial port
8. Determine the type of the serial port (the options vary with the gateway model)
9. Choose the baud rate
10. The data bit in communication (8 bits for RTU communication by default)
11. There are three parity bits, one even parity, one odd parity, and one non-parity bit
12. The stop bit represents the last bit in a single package, and the typical value includes 1, 1.5 and 2

After configuration of the protocol channel, the protocol will be displayed on the page. You can make subsequent changes to the channel like deletion or edition.



Description of the numbered areas

1. Delete the channel or access the detail page of the channel and make changes accordingly, including disabling the channel
2. The channel is set to refresh automatically every 5 seconds, and you can assign an optional value between 1 and 99 for auto refreshing
3. Add a device for data collection

4.2.2 Device Configuration

To add a target PLC to the web interface, first connect the PLC to the gateway, then input the device information in the pop-up window upon a click on the **Add** button as shown in the screenshot above.

The device information to be input varies with the protocol you added for communication.

Take Siemens S7-200 Smart PLC for example, if you apply Ethernet communication, you have to make sure **S7 protocol** is included in the .ipk file and you have created a channel for the protocol. Then you can proceed with the PLC setup under the channel.

Add [X]

① * Device Type: s7_200 smart

② * Device Name: S7

③ * Enabled: YES

④ * Interval_ms: 1000

⑤ * Ip Address: 192.168.19.254

⑥ * Port: 102

⑦ * rack: 0

⑧ * slot: 1

Description of the numbered areas

1. Select the type of device you are going to add
2. Enter a device name
3. Choose to enable the device or not
4. Set an interval for data collection
5. Input the IP address of the device
6. The remaining fields could be left as is

4.2.3 Add Variables to the Device

After configuration of the PLC, set up the variables for sub-devices at different nodes of the PLC.

Add variable to device S7 [X]

① * Name: temp

② * Title: SNS A

③ * Group: Default Group

④ * Register Addr Type: Q

⑤ * Register Addr: 5

⑥ * Date Type: BOOL(bit)


⑦ * Bit Bias: 0

⑧ * Data calculation: none

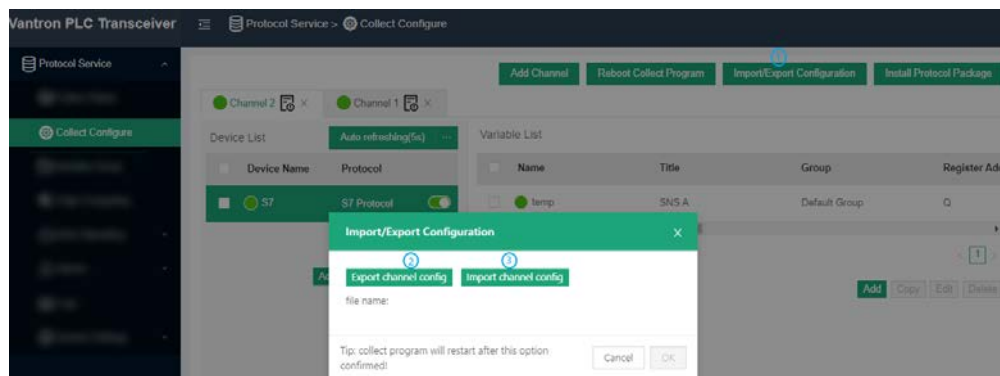
⑨ Import from CSV file ⑩ Download Template Cancel OK

Description of the numbered areas

1. Input a variable name for the sub-device connected to the PLC for data collection
2. Enter a title to describe the variable
3. Set a group for the variable
4. Select the register address type
5. The register address ranges from 1 to 65535
6. The type of data collected is Boolean by default
7. Set a bit bias for the Boolean data type
8. Set a method for data calculation
9. You can skip the fields above and upload a csv file for bulk setup of the variables
10. The csv template demonstrates the compulsory fields


 The register address type and data type are subject to the protocol selected and the type of the PLC.

After configuration of the PLC and the variables at different nodes, you can export the configurations to the local for backup, or, you can import the configurations backed up earlier.



Description of the numbered areas

1. Click **Import/Export Configuration** to access the page
2. Export the channel configurations to the local
3. Import the channel configurations from the local

 Exporting the configurations will back up the configurations of every single channel on the page.

4.2.4 Edge Computing Scripts Setup

To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, and input the script information in the pop-up window upon a click on **Add Script**.

Add Script

Script Name: Engine: Enable: ☒

Variable Name:	Execute Object
DBW03	hmdty
DBW04	PLC-2
DBW05	temp

```

1 function toInt(v)
2 {
3   return !!v ? 1:0;
4 }
5
6 bool_gg_10 - !!DBW03;
7 bool_gg_11 - !(toInt(DBW03) ^ toInt(DBW04));
8 bool_gg_12 - !(toInt(DBW04) ^ toInt(DBW05));
  
```

Compute Result:	Data Type:
bool_gg_10	Bool
bool_gg_11	Bool
bool_gg_12	Bool

Description of the numbered areas

1. Edit the input variable: add a name for the input variable and an object for executing the script (more than one variable could be added)
2. Edit the output variable: add the computation result and data type
3. Set the script name
4. Select the format of the script (JavaScript and Lua supported)
5. Compile the script in the window

After compilation, click **OK** to exit. When you put the cursor on the object of a script, information about the variable name and execution object of the script will be available.

Scripts List

<input type="checkbox"/> scriptName	Execute Object	Execute Strategy
<input type="checkbox"/> greetings	[1]	Timed Execution
<input type="checkbox"/> edge computing	Variable Name: DBW03, Execute Object: Channel 2/S7/hmdty	Timed Execution
<input type="checkbox"/> edge computing_1	DBW04, Channel 1/PLC-2	Timed Execution
<input type="checkbox"/> edge computing_2	DBW05, Channel 2/S7/temp	Timed Execution
<input type="checkbox"/> edge computing_2_3	[DBW03,DBW04,DBW05]	Timed Execution

The **Execute Strategy** button above the script list enables to edit the strategy for executing the scripts in bulk.

Execute Strategy

<input type="checkbox"/>	scriptName	Current Strategy	Execute Interval	Reuse Engine
<input type="checkbox"/>	greetings	Timed Execution	1000	Reuse after 100 times execution
<input checked="" type="checkbox"/>	edge computing	Timed Execution	1000	Reuse after 100 times execution
<input checked="" type="checkbox"/>	edge computing_1	Timed Execution	1000	Reuse after 100 times execution
<input checked="" type="checkbox"/>	edge computing_2	Timed Execution	1000	Reuse after 100 times execution

3 scripts selected

* Execute By:

Timed Execution

* Execute Interval:

Timed Execution

ms

* Reuse Engine:

Automatic Execution

The scripts are designed to be executed automatically or at a scheduled time.

Automatic execution: default, triggered when there is abnormality with the execution object.

Timed execution: the system is scheduled to execute the script every 1000ms by default, and you can adjust the interval.

The operation buttons behind each script allow you to start/pause, copy, edit and delete the script. You can access the script information and the execution log upon a click on the edit button.

Edit script edge computing_2_3

Variable Name

Execute Object

Value

DBW03	humidity	false
DBW04	PLC-2	
DBW05	temp	true

Script Name

edge computing_2_3

Engine

JAVASCRIPT

Enable

☒

1 function toInt(v)

2 {

3 return !v ? 1:0;

4 }

5

6 bool_gg_10 = !!(DBW03);

7 bool_gg_11 = !!(toInt(DBW03) ^ toInt(DBW04));

8 bool_gg_12 = !!(toInt(DBW04) ^ toInt(DBW05));

Compute Result

Data Type

Result

bool_gg_10	Bool	
bool_gg_11	Bool	
bool_gg_12	Bool	

Edge computing log

1488 | 2022-03-02 10:21:40 execute: end execute

1489 | 2022-03-02 10:21:41 execute: start to execute compute_c

1490 | 2022-03-02 10:21:41 execute: input DBW04 not ready

1491 | 2022-03-02 10:21:41 execute: end execute

1492 | 2022-03-02 10:21:42 execute: start to execute compute_c

1493 | 2022-03-02 10:21:42 execute: input DBW04 not ready

1494 | 2022-03-02 10:21:42 execute: end execute

Execute

Cancel

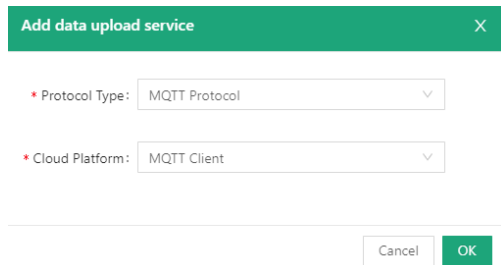
OK

When the setup finishes, you can check the information about the devices and variables under **Collect Status**. Filters are available if you wish to check a specific channel or variable.

5.2.5 Data Upload and Encapsulation

Filed data collected will be uploaded to the cloud platform via protocols after edge computing. Take MQTT protocol as an example, follow the steps below for relevant settings.

- Expand **Data Uploading** tab and click **Upload Config**;
- Click **Add** button at the upper right corner, and select MQTT protocol and MQTT client platform for further configuration ;



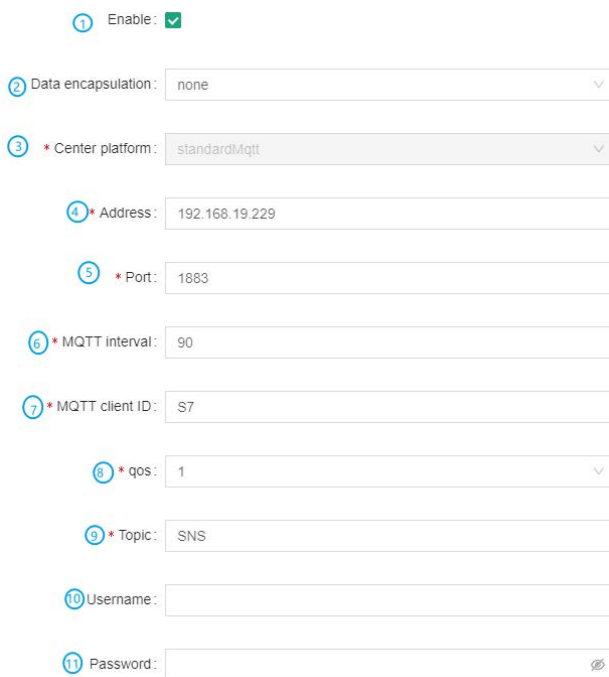
Add data upload service X

* Protocol Type: MQTT Protocol

* Cloud Platform: MQTT Client

Cancel OK

- Configure the MQTT client in the pop-up window.



1 Enable: ☒

2 Data encapsulation: none

3 * Center platform: standardMqtt

4 * Address: 192.168.19.229

5 * Port: 1883

6 * MQTT interval: 90

7 * MQTT client ID: S7

8 * qos: 1

9 * Topic: SNS

10 Username:

11 Password:

Description of the numbered areas

1. Select to enable the protocol after configuration, and the data collected will be automatically uploaded to the cloud platform if enabled
2. Determine the data encapsulation format (no format by default)
3. The center platform is automatically filled and not changeable
4. Fill in the IP address of the cloud platform

5. The port number is automatically filled (1883)
6. The client will send a message to the server within a heartbeat interval, 90 seconds by default and adjustable
7. Input the MQTT client ID
8. Set the quality of service (QoS) to ensure the reliability of the message
 - QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.
 - QoS 1: The message will be sent at least once.
 - QoS 2: The message will be sent only once.
9. Input a topic for the cloud platform
10. Input the name of the cloud platform (non-compulsory)
11. Input the password of the cloud platform (non-compulsory)

The screenshot displays a configuration window with the following steps and fields:

- 12** Enable SSL: ☒
- 13** * Server Certificate: A dropdown menu showing "Customer CA Certificate File".
- 14** * CA Certificate File: A text area containing a long string of base64-encoded data, starting with "HlYmy5QZaCvCudDxoJWMzBiknCAvhToSS3JMFJK" and ending with "-----END CERTIFICATE-----".
- 15** Client Certificate: ☒
- 16** * Client Key File: A text area containing a long string of base64-encoded data, starting with "-----BEGIN RSA PRIVATE KEY-----" and ending with "NQX2/iA16NbZKhOfdy6nenVXYDWe/125wVHIe3zHL".
- 17** * Client Certificate File: A text area containing a long string of base64-encoded data, starting with "Q+mxqc+Xsd0/80n5zxNOWe1DhaxZsTjokYvXnNqlvq" and ending with "vbutsDjmiUq4MyJhmE6MV8l".

12. Select to enable SSL or not
13. If SSL is enabled, select a certification mode for the server
14. If Customer CA certificate File is chosen in the prior step, you'll have to upload a certification file from the local
15. Select to activate client certificate or not
16. If yes, you'll need to upload the client key file
17. Client certificate file is also needed

17 * Client Certificate File:

18 Client Key Password:

19 With buffer: ☒

20 * Backend:

21 * Max memory count:

22 * Max memory size: M

23 * Select devices:

18. Input the client key password (non-compulsory)
19. Select to buffer the data or not
20. If yes, you can choose memory or disk as the buffer path
21. The maximum memory entry count is 1000 by default
22. The maximum memory space occupied is 1M by default
23. Select a device for the data source
24. After submission, the protocol is configured for further use

In the Data Encapsulation page, you can upload encapsulated data or configure the encapsulation format of the data.

Protocol Service > Data Uploading > Data Encapsulation

Data Encapsulation List Upload

<input type="checkbox"/>	Name	Description	Build In Or Not	Operation
<input type="checkbox"/>	Two decimals (lua)		Yes	Delete
<input type="checkbox"/>	Two decimals (js)		Yes	Delete

4.2.6 Alarm

Once configured, alarm information will be detailed on **Alarms** page. Under **Alarms > Alarm Config**, you can add alarm rules for the variables and the sub-devices will alarm once the rule is triggered.

Description of the numbered areas


1. Set a name for the alarm rule
2. Select the variable for the alarm rule to be applied to
3. Input the alarm message to be display in case of an alarm
4. Select to enable the alarm rule or not
5. Set the thresholds for triggering the alarm (thresholds will be applied from top down)
6. Set an alarm level (under normal condition, no alarm will be triggered)

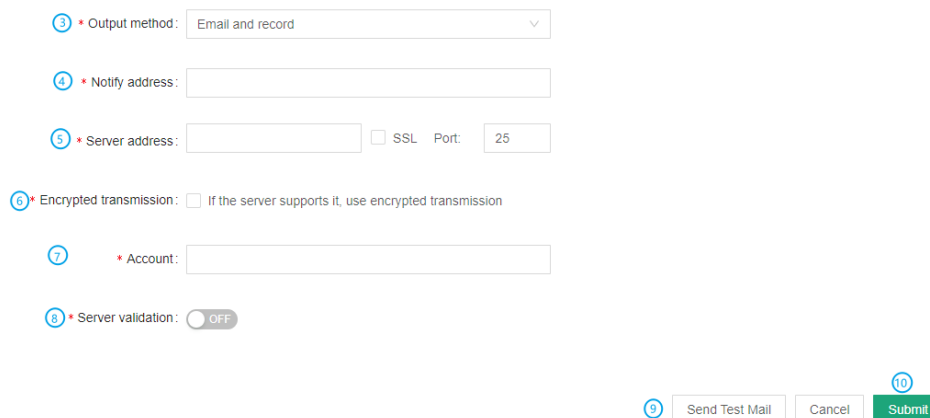
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.

Alarm Broadcast

Description of the numbered areas

1. Set the interval for an alarm, 120 seconds by default
2. The maximum storage space for the alarm log is 1024M by default
3. Select to output the alarms to the alarm log or alarm log + email

 If you choose the latter, please add information about the email.



The screenshot shows a web form for configuring alarm settings. It includes the following elements:

- 3** * Output method: A dropdown menu currently showing "Email and record".
- 4** * Notify address: A text input field.
- 5** * Server address: A text input field, followed by a checkbox for "SSL" and a "Port:" label with a text input field containing "25".
- 6** * Encrypted transmission: A checkbox with the text "If the server supports it, use encrypted transmission".
- 7** * Account: A text input field.
- 8** * Server validation: A toggle switch currently set to "OFF".
- 9** Send Test Mail: A button.
- 10** Submit: A green button.

4. Input an email account for receiving the alarm messages
5. Input the outgoing server address (check the settings of the email server in use)
6. Enable encrypted transmission if the server supports
7. Input an email account for sending the alarm messages (could be same as the receiving email)
8. Toggle the server validation or not
9. Send a test email to check if the settings are ok
10. Submit to apply the settings

When all the rules are set, alarm logs will be displayed on Alarm Record once the rules are triggered.

4.2.7 Logs

Data collection log and cloud service log are displayed on **Logs** page. You can make changes accordingly.

4.2.8 System Settings

Under **System Settings**, you can configure system parameters and check the system information concerned.

CHAPTER 5

DISPOSAL AND WARRANTY

5.1 Disposal

When the device comes to end of life, you are suggested to properly dispose of the device for the sake of the environment and safety.

Before you dispose of the device, please back up your data and erase it from the device.

It is recommended that the device is disassembled prior to disposal in conformity with local regulations. Please ensure that the abandoned batteries are disposed of according to local regulations on waste disposal. Do not throw batteries into fire or put in common waste canister as they are explosive. Products or product packages labeled with the sign of “explosive” should not be disposed of like household waste but delivered to specialized electrical & electronic waste recycling/disposal center.

Proper disposal of this sort of waste helps avoid harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

5.2 Warranty

Product warranty

VANTRON warrants to its CUSTOMER that the Product manufactured by VANTRON, or its subcontractors will conform strictly to the mutually agreed specifications and be free from defects in workmanship and materials (except that which is furnished by the CUSTOMER) upon shipment from VANTRON. VANTRON's obligation under this warranty is limited to replacing or repairing, at its option, of the Product which shall, within **24 months** after shipment, effective from invoice date, be returned to VANTRON's factory with transportation fee paid by the CUSTOMER and which shall, after examination, be disclosed to VANTRON's reasonable satisfaction to be thus defective. VANTRON shall bear the transportation fee for the shipment of the Product to the CUSTOMER.

Out-of-Warranty Repair

VANTRON will furnish the repair services for the Product which are out-of-warranty at VANTRON's then-prevailing rates for such services. At customer's request, VANTRON will provide components to the CUSTOMER for non-warranty repair. VANTRON will provide this service as long as the components are available in the market; and the CUSTOMER is requested to place a purchase order up front. Parts repaired will have an extended warranty of 3 months.

Returned Products

Any Product found to be defective and covered under warranty pursuant to Clause above, shall be returned to VANTRON only upon the CUSTOMER's receipt of and with reference to a VANTRON supplied Returned Materials Authorization (RMA) number. VANTRON shall supply an RMA, when required within three (3) working days of request by the CUSTOMER. VANTRON shall submit a new invoice to the CUSTOMER upon shipping of the returned products to the CUSTOMER. Prior to the return of any products by the CUSTOMER due to rejection or warranty defect, the CUSTOMER shall afford VANTRON the opportunity to inspect such products at the CUSTOMER's location and no Product so inspected shall be returned to VANTRON unless the cause for the rejection or defect is determined to be the responsibility of VANTRON. VANTRON shall in turn provide the CUSTOMER turnaround shipment on defective Product within **fourteen (14) working days** upon its receipt at VANTRON. If such turnaround cannot be provided by VANTRON due to causes beyond the control of VANTRON, VANTRON shall document such instances and notify the CUSTOMER immediately.

Appendix A Regulatory Compliance Statement

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.

APPENDIX B Acronyms

Acronym	Description
RXD	Receive data
TXD	Transmit data
GND	Ground
NC	No connection